airHaul² Nexus PRO™
sB3021

User Guide

Version 1.0

Copyright © smartBridges Pte Ltd. All Rights Reserved.

TABLE OF CONTENTS

ABOUT THIS DOCUMENT **4**

OVERVIEW OF USER GUIDE **4**

RELATED PUBLICATIONS **5**

TECHNICAL SUPPORT CENTER **5**

1. INTRODUCTION **6**

1.1. airHaul² Nexus PRO Configuration Features 6
1.2. System Requirements 6
1.3. Checklists 7

2. AIRHAUL² NEXUS PRO™ CONFIGURATION **11**

2.1. User Login and License Agreement 11
2.2. Web GUI Administrator Password Change 15
2.3. Using the Configuration Pages 16
2.4. Navigation Menu Bar 18
2.5. Device Operation Mode 22
2.5.1 Repeater Mode Configuration 22
2.5.2 Link Aggregate Root Router Mode 25
2.5.3 Link Aggregate Remote Router/NAT Mode 29
2.6 Dual Radio Configuration 32
2.6.1 Root Bridge to Remote Bridge 32
2.6.2 Root Bridge to Remote Router/NAT 34
2.6.3 Remote Bridge to Root Bridge 36
2.6.4 Remote Router/NAT to Root Bridge 37
2.6.5 Remote Router/NAT to Remote Bridge 39
2.6.6 Remote Bridge to Remote Router/NAT 40
2.7 Root Bridge Configuration 43
2.7.1 Bridge IP Configurations 43
2.7.2 Wireless Configurations 44
2.7.3 Configuring Spanning Tree Protocol (STP) 48
2.7.4 STP Settings Configuration 48
2.8 Remote Bridge Configuration 52
2.8.1 Bridge IP Configuration 52
2.8.2 Wireless Configuration 53
2.9 Remote Router/NAT Configuration 55
2.9.1 Bridge IP Configuration 55
2.9.2 Wireless Configuration 56
2.9.3 DHCP Configurations 59
2.9.4 DHCP Relay Configurations 60
2.9.5 Routing Table 62
2.10 Disabling Radio for Single Radio Operation 65
2.11. Wireless Settings Management 67
2.11.1 Wireless Settings 67
2.11.2 Data Encryption 67

3. PERFORMANCE PARAMETERS AND BANDWIDTH CONTROLLER **72**

3.1 LINK PERFORMANCE PARAMETERS AND FEATURES 72
3.2 BANDWIDTH CONTROLLER 75
4. QUALITY OF SERVICE (QOS) 76
5. SURVEY 85
6. ANTENNA ALIGNMENT 86
7. TRAFFIC STATISTICS 88
8. TOOLS 91
8.1 SYSTEM CONFIGURATION 91
8.1.1 SNMP Security 93
8.1.2 Reset Options 94
8.1.3 NTP Time Server Setup 95
8.2 PROFILE MANAGER 95
8.2.1 Save Profile 97
8.2.2 Load Operating Profile 97
8.2.3 Profile Calendar 97
8.3 LINK TEST 99
8.3.1 Throughput Test 100
8.4 LINK BUDGET PLANNING 101
9. FIRMWARE UPGRADE 103
APPENDIX A – POINTS TO REMEMBER 105
APPENDIX B – USEFUL TERMS AND DEFINITIONS 108
APPENDIX C – SNMP TRAP 111
APPENDIX D – SNMP MIB 112
APPENDIX E – LICENSE 113

About This Document

This User Guide is for the networking professional who configures and manages the smartBridges' Intelligent Nexus wireless backhaul, the airHaul^2 Nexus PRO™.

It provides detailed information on using the web-based configuration GUI to configure the airHaul^2 Nexus PRO unit. This manual will help you gain a better understanding of how the various components of Nexus work.

To configure smartBridges' products, you need to have a fundamental understanding of the concepts and technology of Local Area Networks (LAN) and wireless networking. The system installer will require expertise in the following areas:

- Outdoor radio equipment installation
- Network configuration
- Use of web browser for system configuration, monitoring and fault finding

In this chapter, you will find an overview of the User Guide and where to obtain additional information regarding installation and set-up.

Overview of User Guide

The airHaul^2 Nexus PRO (sB3021) User Guide provides information on how to set-up and deploy the unit. A web-based management tool is provided to assist the user to configure the airHaul^2 Nexus PRO unit for different purposes.

In chapter 1, the configuration features of the web-based management tool and the system requirements are listed.

Chapter 2 explains how to login as an administrator and to change the default password. The features of the configuration page as well as the Navigation Menu Bar are explained. You will also learn how to configure the unit to Repeater mode and to convert from one mode to the other. Also in this chapter, instructions on modifying the configurations of the device such as Ethernet, Wireless, Bandwidth, Radio parameters, Throughput Optimizer and Spanning Tree Protocol (STP) are given. Similar instructions are provided for the Repeater or Link Aggregate (individual radio can be in Remote Bridge, Remote Router/NAT). Finally, details on managing the wireless settings are provided.

Functions common to the different modes such as Link Performance parameters and Bandwidth Controller are explained in chapter 3.

Chapter 4 explains the steps for configuring the Quality of Service (QoS) for the aH^{2}NP.

The Site Survey Tool is explained in Chapter 5 and Chapter 6 shows how to perform antenna alignment to optimize the radio performance.

Chapter 7 illustrates how to display Wireless and Ethernet Traffic Statistics through the 'Networking' | 'Statistics' drop down menu

The System Configuration such as modifying the SNMP security settings and resetting the unit are given in Chapter 8. You will also learn how to save the configuration parameters as profiles and using the Link Budget Planning Tool.

Finally, chapter 9 shows how to upgrade the airHaul^2 Nexus PRO through the web management interface to the latest firmware.

Related Publications

These documents provide complete information about the Nexus series of radio units:

- Quick Install Guide (QIG)
- Release Notes
- Technical Specification

All the information can also be found on our website at http://www.smartbridges.com/

Technical Support Center

Comprehensive technical support by dedicated smartBridges engineers is available to all customers through the smartBridges support center website. The website provides updated tools and documents to help troubleshoot and resolve technical issues related to smartBridges products and technologies. To access the technical support resources, please visit the support center website at http://www.smartbridges.com/support/

You will need to register for certain services and downloads on the smartBridges support center website.

1. Introduction

In this chapter, the configuration features of the web-based management tool and the system requirements are listed.

1.1. airHaul^2 Nexus PRO Configuration Features

The airHaul^2 Nexus PRO web-based management tool provides the user with the following features:

1. System configuration
2. Device operational mode configuration
3. Ethernet and wireless IP configurations
4. Security
5. Radio (SSID, domain, channel, etc) parameter configuration
6. Network bridge (STP, etc) parameter configuration
7. Bandwidth management
8. QoS
9. Antenna alignment
10. Traffic Statistics
11. Site Survey
12. Profile management
13. User management
14. Link Test
15. Link Budget Planning Calculator
16. Firmware Upgrade

1.2. System Requirements

The following are the minimum system requirements for the airHaul^2 Nexus PRO™ web-based configuration management tool:

1. Operating System: either Windows 98/2000/XP/NT or Linux

2. Connection to the internet for downloading the latest firmware and Sun Java

3. Web browser: either Internet Explorer 5.0 and higher, Netscape 7.2 and higher, Mozilla 1.7 and higher or Mozilla Firefox 0.8 and higher

4. SUN JRE: v1.5 and above. You may download it from http://java.sun.com/j2se/1.5.0/download.jsp

Please visit http://www.smartbridges.com/ for the latest information and updates.

1.3. Checklists

Pre-Installation Checklist for airHaul^2 Nexus PRO

Organization Name/Site Name	
Address	
City	
State	
Zip Code	
Telephone Number	

Site Survey and Link Planning				
No	**Parameters**	**Units**	**Site A**	**Site B**
1	Regulatory Standard to be followed	For example, FCC/ETSI		
2	Frequency Band (in GHz)	2.4 5.25-5.35 5.47-5.725 5.725-5.805		
3	Maximum Output Power as per the Regulatory Authority	100mW/1W/4W		
4	Latitude	Deg Min Sec		
5	Longitude	Deg Min Sec		
6	UPS Installed	Yes/No		
7	UPS specification if any	KVA		
8	Line Voltage	90V-264V AC,50-60 Hz		
9	Near Line of site between sites	Yes/No		
10	Height of tower	Feet/Meters		
11	Repeater required to achieve a link	Yes/No		
12	If Repeater required, then reason why	For example, to achieve long distance/LoS etc		
13	No. of repeaters required	Number		
14	Required Throughput	Mbps		
15	Distance between sites	Miles/km		
16	Antenna Type	Parabolic/sector		
17	Antenna Mfg.	smartBridges/Name of other manufacturer		
18	Gain of antenna	dBi		
19	Antenna Polarization	Horizontal/Vertical		
20	Beam width of antenna	Horizontal – deg		
		Vertical – deg		
21	Type of external cable type	LMR 400/LMR600/etc		

No	Parameters	Units	Site A	Site B
22	Length of external cable connecting a Radio and antenna	Feet/meters		
23	Fade Margin taken into account for a link budgeting	Ideally between 10 to 20 dBm		
24	Model of smartBridges equipment selected for a link	sB3021		
25	Grounding- Earth to Neutral Voltage	Ideally less than 2 Volts		
26	Length of the Ethernet cable required for powering a unit	Feet/meters		
27	Choose the best channel which can be used on the basis of site survey with help of scanning tools such as Netstumbler	Specify channel number		

Pre Installation Lab Testing of Equipment				
No	**Parameters**	**Units**	**Site A**	**Site B**
1	Network diagram along with IP address of all the interfaces for link to be setup in Place	Yes/No		
2	Availability of Quick Installation Guide	Yes/No		
3	Availability of User guide and CD	Yes/No		
4	Ensure that all items listed in the "Package Contents" of Quick Installation Guide are included in the shipment	Yes/No		
5	Availability of Installation Kit	Yes/No		
6	Radio MAC address of airHaul^2 Nexus PRO	Yes/No		
7	Settings configured for pre-installation testing	Yes/No		
8	Ping response	ms		
9	Ping Success Rate	Percentage %		
10	Throughput test (Upload/Download)	Varies depending on signal strength, link quality and distance		

Signature of Engineer:	
Name:	
Email:	
Date:	

Post-Installation Checklist for airHaul^2 Nexus PRO

Organization Name/Site Name	
Address	
City	
State	
Zip Code	
Telephone Number	

General Configuration Information				
No	**Parameters**	**Units**	**Site A**	**Site B**
1	Radio Operation Mode	Repeater or Link Aggregate		
2	Mode of Operation	PTP		
3	SSID of a Radio	Up to 32 characters		
4	IP address of Ethernet Port	32-bit numeric address		
5	IP address of Wireless Port (for Router mode)	32-bit numeric address		
6	Noise Floor	dBm		
7	RSSI	dBm		
8	Channel selected for Link	Channel No		
9	Radio TX Output Power	-5 to +23dBm		
10	Antenna Gain	dBi		

Checklist				
No	**Parameters**	**Units**	**Site A**	**Site B**
1	Check out the crimping of the Ethernet cable at both the ends	Yes/No		
2	Check out the proper grounding of the antenna and equipment	Yes/No		
3	Ensure no extreme bends or kink's in the cable	Yes/No		
4	Ensure Ethernet cable is not running near a sharp edge	Yes/No		
5	Ensure airHaul^2 Nexus PRO along with antenna is fixed securely on a tower/mast with the help of nuts and bolt supplied in packaging	Yes/No		
7	Ping response	ms		
8	Ping success rate	Percentage		
9	Throughput test (Upload / Download)	Mbps		
10	Link stability based on observation for 1 Hr	Yes/No		

Signature of Engineer:	
Name:	
Email:	
Installation Date:	
Commissioned Date:	

For the latest information on smartBridges products, please visit our website at: http://www.smartbridges.com/

2. airHaul^2 Nexus PRO™ Configuration

Here you will learn how to login as an administrator and to change the default password to one of your choice. The features of the configuration page as well as the Navigation Menu Bar are explained. You will also learn how to configure the dual radios to the desired mode and to convert from one mode to the other.

Also in this chapter, instructions on modifying the configurations of the Root Bridge such as Ethernet, Wireless, Bandwidth Control, radio performance parameters, Throughput Optimizer and Spanning Tree Protocol (STP) are given. Similar instructions are provided for the Remote Bridge and Remote Router/NAT.

Finally, details on managing the wireless settings are provided.

2.1. User Login and License Agreement

The airHaul^2 Nexus PRO unit comes with the pre-configured default Ethernet (wired-side) IP address: **192.168.0.208** and subnet mask: 255.255.255.0. This default device IP address should be used when accessing the device configuration management interface for the first time using a web-browser (Enter **http://192.168.0.208** for the URL address). In addition, the Sun Java Plug-in should be installed. The PC must be on the same subnet as the unit.

Follow the steps below to login as an Administrator to the web-based configuration management interface system:

1. Connect the radio using the Power over Ethernet (PoE) to a PC or network via the ETH A or ETH B port (Please refer to the Quick Install Guide for more information on connections).

2. Open a web browser on the PC and enter the device's IP address **192.168.0.208** in the web browser address field and press Enter.

3. A user login box will appear. Enter the **'User name**' and **'Password'** and check the 'Remember my password' checkbox if you want the system to remember the password. The default user name is **Administrator** and the password is **smartBridges** (case sensitive).

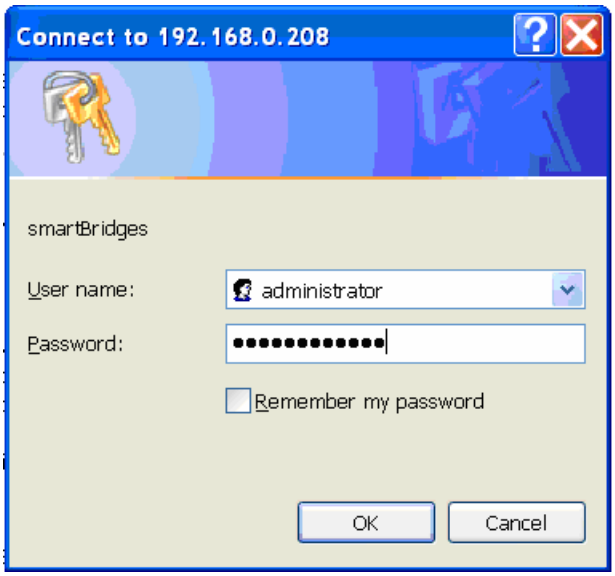


Figure 2-1 Administrator Login

4. Click the **'OK'** button. A License agreement page will appear as shown in Fig 2-2 below.

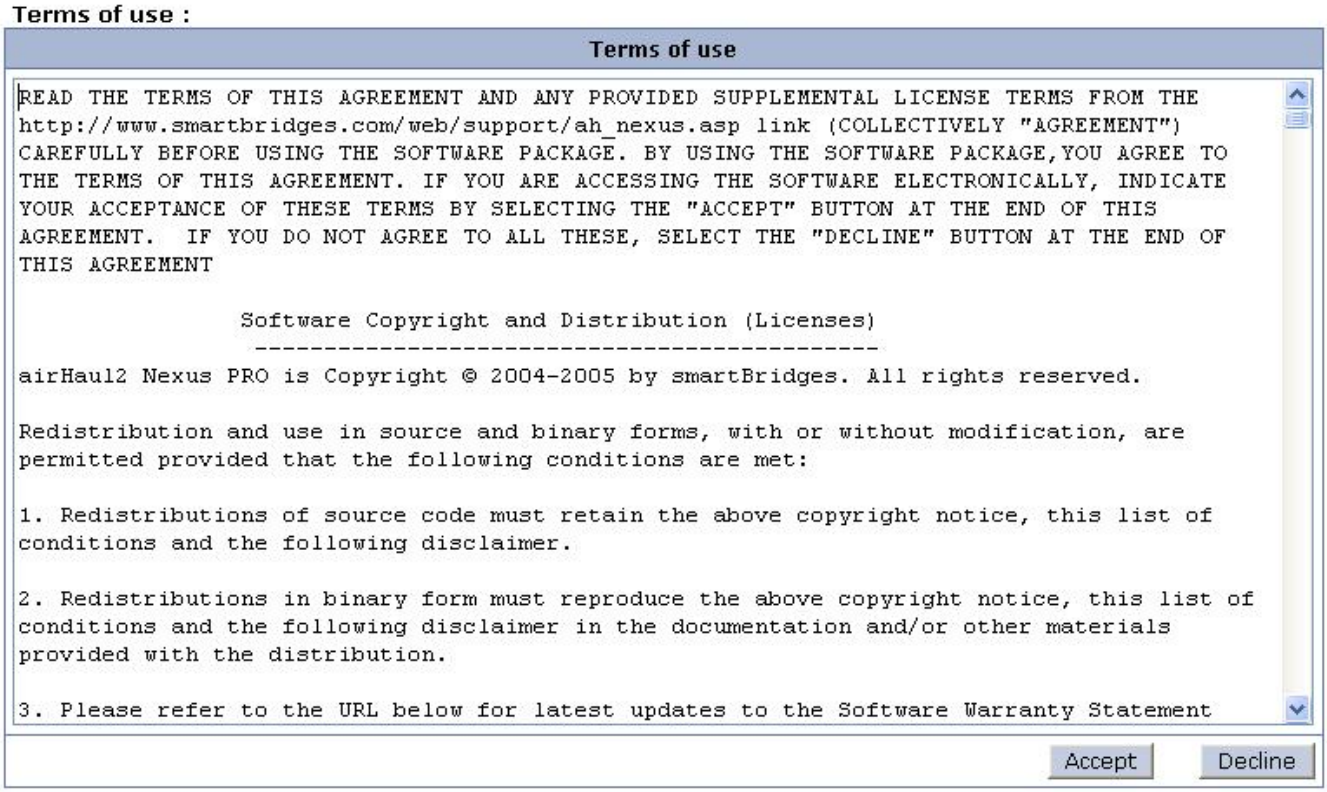
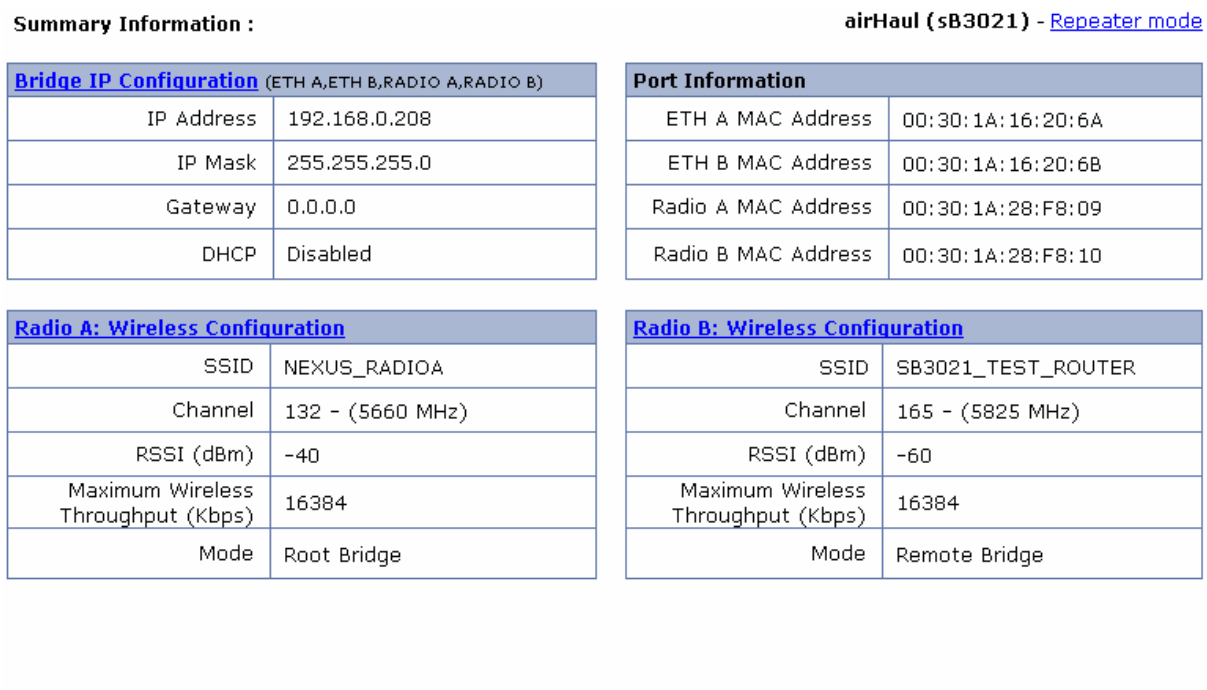

Terms of use :
Terms of use
READ THE TERMS OF THIS AGREEMENT AND ANY PROVIDED SUPPLEMENTAL LICENSE TERMS FROM THE http://www.smartbridges.com/web/support/ah_nexus.asp link (COLLECTIVELY "AGREEMENT") CAREFULLY BEFORE USING THE SOFTWARE PACKAGE. BY USING THE SOFTWARE PACKAGE,YOU AGREE TO THE TERMS OF THIS AGREEMENT. IF YOU ARE ACCESSING THE SOFTWARE ELECTRONICALLY, INDICATE YOUR ACCEPTANCE OF THESE TERMS BY SELECTING THE "ACCEPT" BUTTON AT THE END OF THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL THESE, SELECT THE "DECLINE" BUTTON AT THE END OF THIS AGREEMENT
Software Copyright and Distribution (Licenses)
airHaul2 Nexus PRO is Copyright © 2004-2005 by smartBridges. All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Please refer to the URL below for latest updates to the Software Warranty Statement
Accept
Decline

Figure 2-2 License Agreement Page

5. Click **'Accept'**. The airHaul^2 Nexus PRO Nexus Summary Information' page (Fig 2-3) will appear.



Summary Information : **airHaul (sB3021)** - Repeater mode

Bridge IP Configuration (ETH A,ETH B,RADIO A,RADIO B)	
IP Address	192.168.0.208
IP Mask	255.255.255.0
Gateway	0.0.0.0
DHCP	Disabled

Port Information	
ETH A MAC Address	00:30:1A:16:20:6A
ETH B MAC Address	00:30:1A:16:20:6B
Radio A MAC Address	00:30:1A:28:F8:09
Radio B MAC Address	00:30:1A:28:F8:10

Radio A: Wireless Configuration	
SSID	NEXUS_RADIOA
Channel	132 - (5660 MHz)
RSSI (dBm)	-40
Maximum Wireless Throughput (Kbps)	16384
Mode	Root Bridge

Radio B: Wireless Configuration	
SSID	SB3021_TEST_ROUTER
Channel	165 - (5825 MHz)
RSSI (dBm)	-60
Maximum Wireless Throughput (Kbps)	16384
Mode	Remote Bridge

Figure 2-3 airHaul2 Nexus PRO Summary Information Page

The page information descriptions are provided in the table below.

Table 2-1 Page Information Descriptions

Page Item		Descriptions
Bridge IP configuration	IP Address	Editable Ethernet IP Address.
	IP Mask	Editable Ethernet IP subnet Mask
	Gateway	Editable Gateway IP address.
	DHCP	Editable DHCP status Disabled/Enabled The user can enable DHCP by ticking the check box to obtain an IP address from the network DHCP server
Radio A Wireless Configuration	SSID	Device SSID.
	Channel	Device operation channel.
	RSSI	RSSI value when associated
	Maximum Wireless Throughput	Maximum Wireless Throughput in kbps for Radio A
	Mode	Displays current operational mode of the radio
Radio B Wireless Configuration	SSID	Device SSID
	Channel	Device operation channel.
	RSSI	RSSI value when associated
	Maximum Wireless Throughput	Maximum Wireless Throughput in kbps for Radio B
	Mode	Displays current operational mode of the radio
Port Information	ETH A MAC Address	Ethernet A (wired side) MAC address. Display only
	ETH B MAC Address	Ethernet B (wired side) MAC address. Display only
	Radio A MAC Address	Radio A MAC address. Display only
	Radio B MAC Address	Radio B MAC address. Display only
Device Operational Mode	Device operational mode	Current device operational mode is displayed in the top right corner. It could be Repeater Mode, Link Aggregate Root Router Mode, Link Aggregate Remote Router/NAT Mode.

2.2. Web GUI Administrator Password Change

By default the Administrator password is **smartBridges** (case sensitive).

Follow the steps below to change the Administrator password.

1. Click on the **'Tools | User Manager'** drop down menu in the navigation menu bar. An 'Administrator Password change' GUI will appear.
2. Enter the fields **'Old Password'**, **'new Authentication Password'** and **'Confirm new Authentication Password'** as shown in Figure 2-4.
3. Click on the **'Apply Changes'** button to effect the password change.

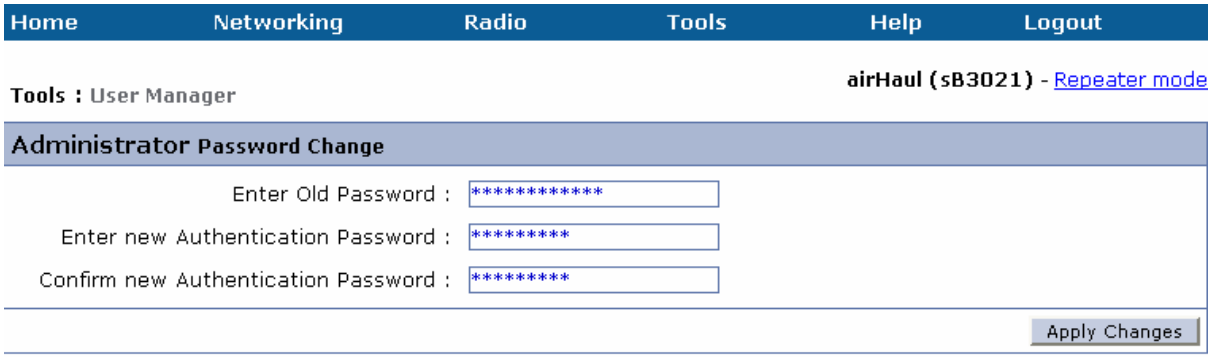
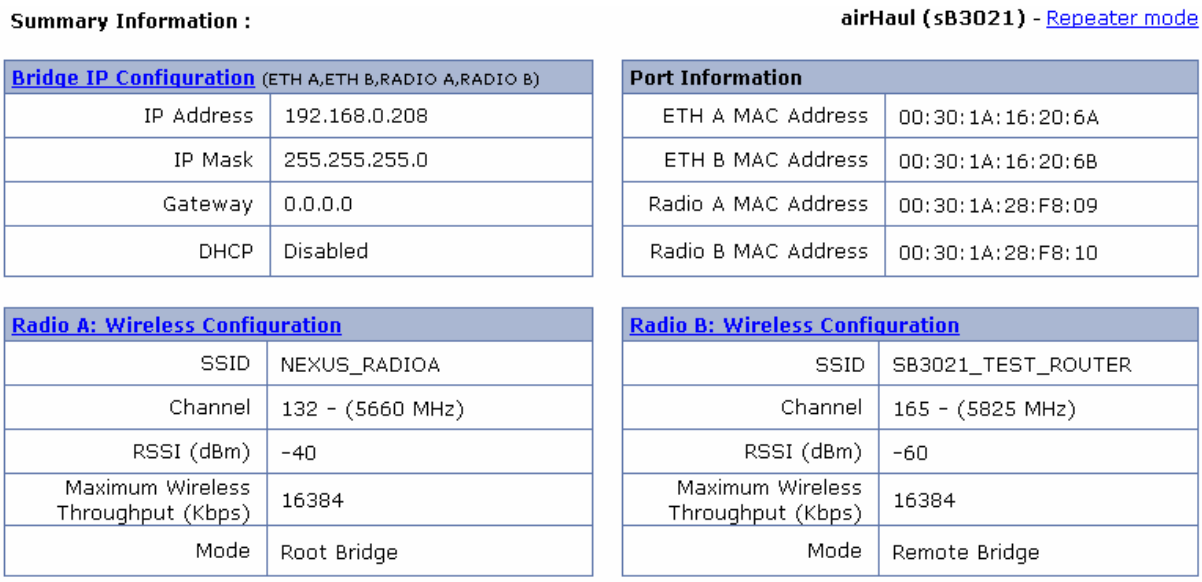


Figure 2-4 Administrator password change

2.3. Using the Configuration Pages

The airHaul^2 Nexus PRO configuration system comprises of several pages for configuring the various parameters. A common navigation menu bar is provided at the top of each page for easy navigation as shown in the figure below.



Summary Information : **airHaul (sB3021)** - Repeater mode

Bridge IP Configuration (ETH A,ETH B,RADIO A,RADIO B)	
IP Address	192.168.0.208
IP Mask	255.255.255.0
Gateway	0.0.0.0
DHCP	Disabled

Port Information	
ETH A MAC Address	00:30:1A:16:20:6A
ETH B MAC Address	00:30:1A:16:20:6B
Radio A MAC Address	00:30:1A:28:F8:09
Radio B MAC Address	00:30:1A:28:F8:10

Radio A: Wireless Configuration	
SSID	NEXUS_RADIOA
Channel	132 - (5660 MHz)
RSSI (dBm)	-40
Maximum Wireless Throughput (Kbps)	16384
Mode	Root Bridge

Radio B: Wireless Configuration	
SSID	SB3021_TEST_ROUTER
Channel	165 - (5825 MHz)
RSSI (dBm)	-60
Maximum Wireless Throughput (Kbps)	16384
Mode	Remote Bridge

Figure 2-5 Navigation Menu Bar

The system configuration information is displayed as read-only in each page. As shown in the '**Summary Information**' page above, **Bridge IP Configuration**', 'Wireless Configuration for Radio A and Radio B' are configurable. The 'Port Information' parameters are displayed as read only.

Clicking on the parameter heading allows you to edit the configuration parameters. To change the Bridge IP, click on the '**Bridge IP Configuration**' link. Similarly, clicking on the '**Wireless Configuration**' link the 'Radio Configuration page for the particular radio either Radio A or Radio B' will be displayed to edit any wireless settings. The figure below shows the 'Bridge IP Configuration' parameters in editable boxes.

To save the changes to the system, you need to click on the '**Apply Changes**' button.

Summary Information :

airHaul (sB3021) - Repeater mode

Bridge IP Configuration (ETH A,ETH B,RADIO A,RADIO B)	
IP Address	192.168.0.208
IP Mask	255.255.255.0
Gateway	0.0.0.0
DHCP	Disabled

Port Information	
ETH A MAC Address	00:30:1A:16:20:86
ETH B MAC Address	00:30:1A:16:20:87
Radio A MAC Address	00:30:1A:28:F6:B2
Radio B MAC Address	00:30:1A:28:F6:B3

Radio A: Wireless Configuration	
SSID	NEXUS_RADIOA
Channel	132 - (5660 MHz)
RSSI (dBm)	No Association
Maximum Wireless Throughput (Kbps)	30720
Mode	Root Bridge

Radio B: Wireless Configuration	
SSID	NEXUS_RADIOB
Channel	153 - (5765 MHz)
RSSI (dBm)	No Association
Maximum Wireless Throughput (Kbps)	30720
Mode	Remote Bridge

Figure 2-6 Editable Boxes for Parameter Editing

2.4. Navigation Menu Bar

The Navigation Menu Bar contains menu items that allow the user to go to different configuration pages. The following table summarizes the functions available for each of the menu item links.

Table 2-2 Menu Functions

Menu Item	Menu Sub-items	Description
Home	Summary Information	Displays summary page with information such as Bridge IP and Wireless IP settings. Allows user to set the IP settings for Ethernet (wired side) and Wireless interfaces depending on the device operational mode.
Networking	Bridge Configuration	Displays the bridge address, generic bridge port table, spanning tree port table for ports ETH A, ETH B, Radio A., Radio B etc. Bridge configuration option is available when airHaul^2 Nexus PRO is configured in Root Bridge or Remote Bridge mode
	DHCP Server	Configure DHCP server or Relay DHCP option is available only if airHaul^2 Nexus PRO is configured in Remote Router/NAT mode
	Traffic Statistics	Displays the Ethernet and Wireless Traffic Statistics
	Bandwidth Controller	Allows bandwidth management of the wireless link on egress traffic.
	Routing Table	Allows user to view, add and delete static routes. Routing table is available for all the operating modes.
	QoS	The primary goal of QoS is to provide priority including dedicated bandwidth, controlled jitter and latency (required by some real-time and interactive traffic), and improved loss characteristics.
Radio	Radio A Radio B	Wireless Settings: Allows user to set SSID, Channel, ACL Controls and Country, as well as Dial-a-Power.

Menu Item	Menu Sub-items	Description
		Provides a link to view associations. Security: Allows user to set the WEP Keys and to choose between Open/Shared System modes of authentication. **WPA-PSK (TKIP, AES)** is where encryption keys are automatically changed (called **rekeying**) and authenticated between devices after a specified period of time, or after a specified number of packets has been transmitted. **WPA2-PSK (TKIP,AES)** Based on the 802.11i standard, WPA2 was released in 2004 and uses a stronger method of encryption
Tools	System Configuration	System Name: Allows user to change the name of the airHaul^2 Nexus PRO unit System Description: Allows user to enter a description of the airHaul^2 Nexus PRO unit SNMP Security: Allows user to set the SNMP Community String and SNMP Access Filters Reset: Resets the device remotely Delayed Reset: Schedules delayed reset NTP Server : Allows user to change NTP Server Settings Firmware Version: Shows current firmware version
Tools	System Configuration	Radio Firmware Version: Shows current radio firmware version Reset to Defaults: Resets the device with factory defaults

Menu Item	Menu Sub-items	Description
		Ethernet MTU Size: Allows user to set the Ethernet MTU size for different applications. Syslog server IP Address: Allows user to set the Syslog server IP and log level. SNMP Trap server IP Address: Allows user to set the SNMP Trap server IP for SNMP trap forwarding. Watch Guard: The Radio Defenders will monitor the Wireless Association Status (automatically) and traffic and take corrective action if needed. Radar Scan: The Radar Scan can be enabled /Disabled. LED Control Allows user to turn on/off LED control. Device Mode Set the Current Device Operational mode Repeater Mode, Link Aggregation Root Router Mode, Link Aggregation Remote Router/NAT Mode.
	Profile Manager	Save Profile Allows user to define and save up to three device operating profiles for easy device management. The installation profile is always available. Operating Profile Allows user to load the profile from saved profiles and shows last loaded profile Profile Calendar Allows user to plan and manage the use of different profiles at different times efficiently.
	Link Test	Allows user to do a throughput test and ping test. These tools could be very helpful during the installation phase.
	Link Budget Planning Calculator	Allows user to calculate the Link Budget.

Menu Item	Menu Sub-items	Description
Tools	Antenna alignment	Shows the link status, link quality, RSSI. This menu item is available when airHaul^2 Nexus PRO is configured in Remote Bridge mode or Remote Router/NAT mode
	Site Survey	Shows all the wireless devices operating in the area. This menu item is available when airHaul^2 Nexus PRO is configured in Remote Bridge mode or Remote Router/NAT mode.
	User Manager	Allows the administrator to change the Administrator password.
	Firmware Upgrade	Allows user to update to new firmware versions.
Help	Technical Support	Information on Technical Support
	User Guide – Online	Links to online user guide
	Product registration and feedback	Allows user to register the product and provide feedback or suggestions.
	Check for updates	Checks smartBridges website for any software updates.
	About airHaul^2 Nexus PRO	General system description, software version information and warranty information.

2.5. Device Operation Mode

This section explains the configurations possible in the different modes. With dual radios, the airHaul^2 Nexus PRO allows for maximum operation flexibility.

2.5.1 Repeater Mode Configuration

Normally, to extend the WLAN coverage of an access point, a repeater site with 2 single radio backhauls will be used in a Root and Remote combination. This results in a degradation of the link efficiency which could be due to several reasons: a single link with larger spacing gives lower bandwidth, the Remote might not be in line of sight, etc.

However, with the dual radio airHaul^2 Nexus PRO configured in Repeater Mode, it is possible to extend WLAN coverage while still maintaining a higher bandwidth.

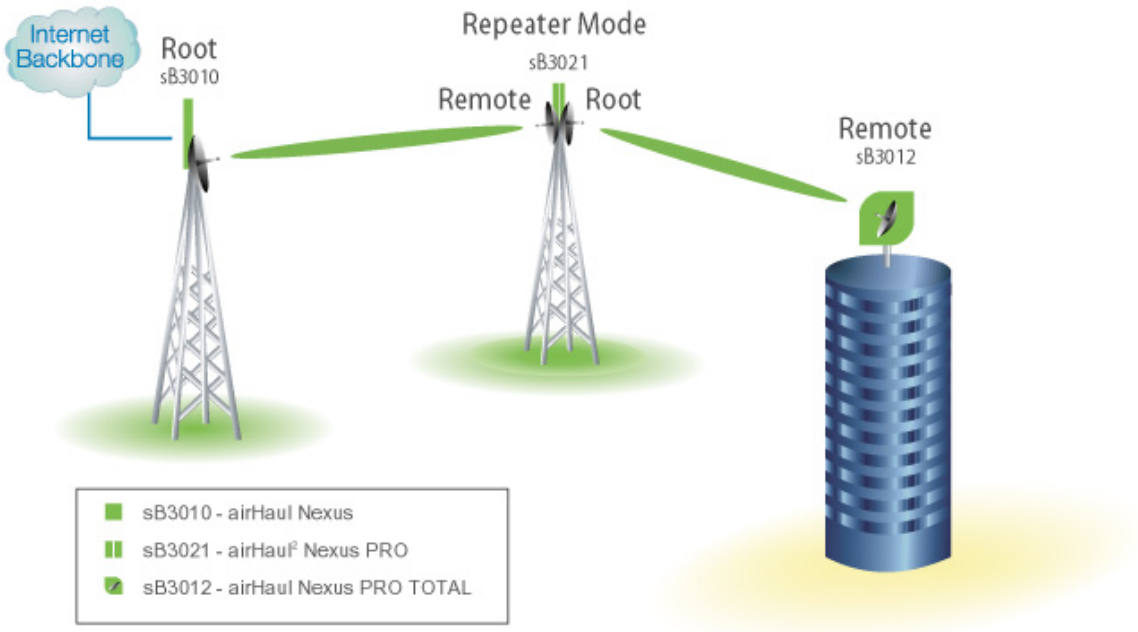


Figure 2-7 Repeater Mode

In the above diagram, we see that the airHaul^2 Nexus PRO configured in Root Bridge Mode is servicing an Internet backbone. One radio (Radio A) is configured as Root and the other radio (Radio B) is configured as a Remote Bridge or Remote Router/NAT. In such a scenario, the backhaul link can span up to 50 miles (80 km).

To configure the device in Repeater Mode, follow the steps below:

1. Go to Tools | System Configuration dropdown Menu. The **System Configuration** will be displayed as shown below.
2. Click on the **Device Mode** link in the **System Configuration** page.
3. Choose **Repeater Mode** option and click on **Apply Changes**. Two dropdown menus for configuring the two radios will appear.
4. Radio A can be configured as Root and Radio B as Remote and vice versa.
5. Click on **Apply Changes**. A confirmation IP configuration pop up window will appear as shown below.
6. Click on the **Apply Changes** to save the IP configuration.
7. Please wait for the device to regain the settings in the Repeater Mode before proceeding to configure the appropriate radio in the Root and Remote Mode.

Note: Please refer to the Radio Configuration Section for configuring one radio as Root and the other as Remote.

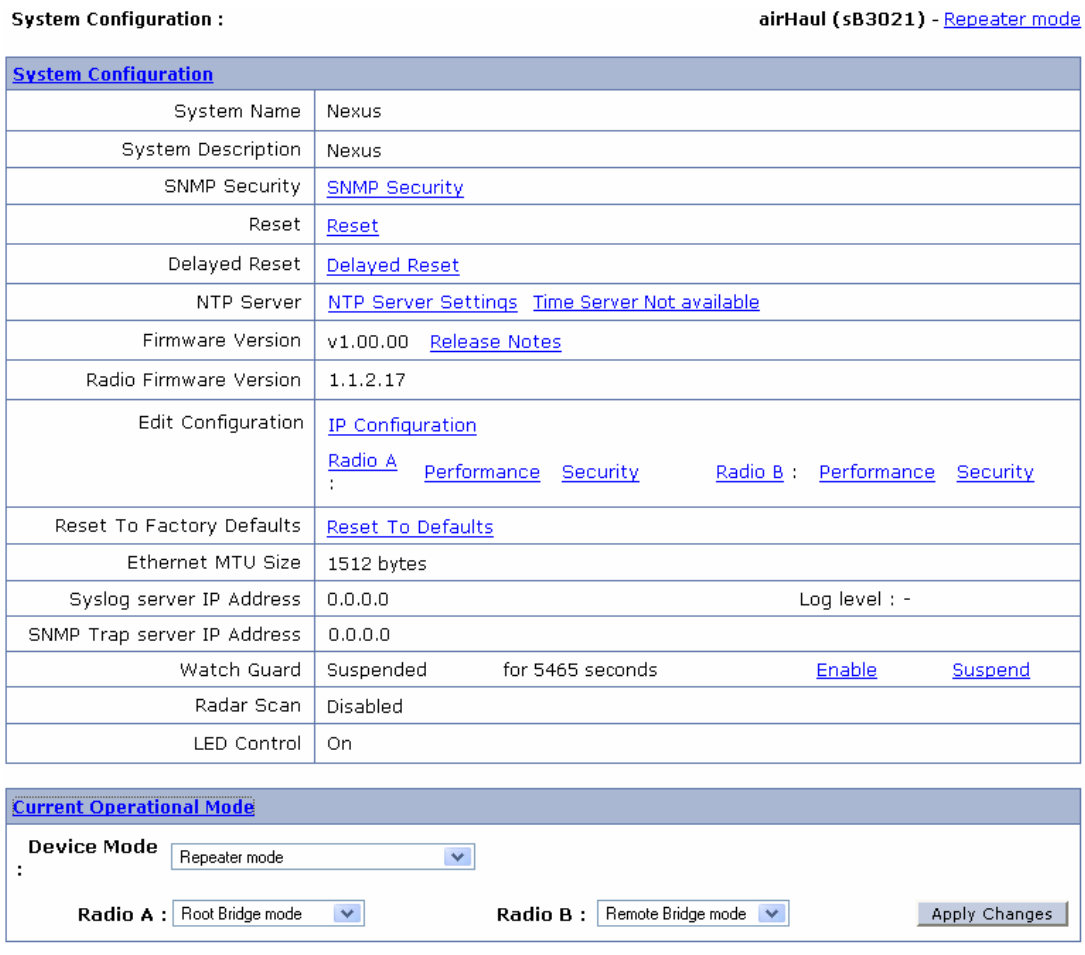


Figure 2-8 Repeater Mode Selected

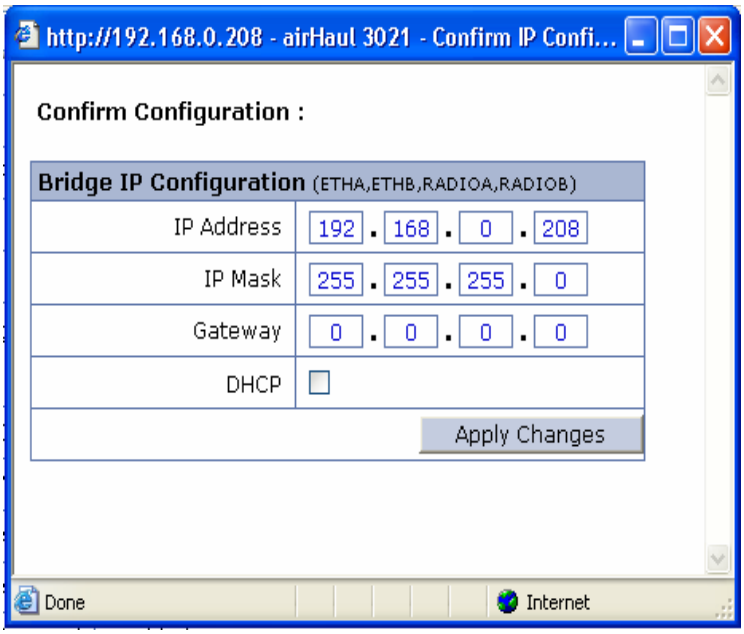


Figure 2-9 Confirmation IP Configuration

Summary Information :

airHaul (sB3021) - Repeater mode

Bridge IP Configuration (ETH A,ETH B,RADIO A,RADIO B)	
IP Address	192.168.0.208
IP Mask	255.255.255.0
Gateway	0.0.0.0
DHCP	Disabled

Port Information	
ETH A MAC Address	00:30:1A:16:20:86
ETH B MAC Address	00:30:1A:16:20:87
Radio A MAC Address	00:30:1A:28:F6:B2
Radio B MAC Address	00:30:1A:28:F6:B3

Radio A: Wireless Configuration	
SSID	NEXUS_RADIOA
Channel	132 - (5660 MHz)
RSSI (dBm)	No Association
Maximum Wireless Throughput (Kbps)	30720
Mode	Root Bridge

Radio B: Wireless Configuration	
SSID	NEXUS_RADIOB
Channel	153 - (5765 MHz)
RSSI (dBm)	No Association
Maximum Wireless Throughput (Kbps)	30720
Mode	Remote Bridge

Figure 2-10 Repeater Mode with both radios associated

2.5.2 Link Aggregate Root Router Mode

The Link Aggregate Mode is used to achieve increased bandwidth, high availability and link redundancy. Link aggregation is used to optimize port (link) usage by grouping ports (Radio A and Radio B) together to form a single aggregate link with a higher bandwidth.

The Link Aggregate Mode also provides link redundancy without user intervention if one of the link fails. However, please note that if one of the links fail, the bandwidth will be reduced as only a single link is functional.

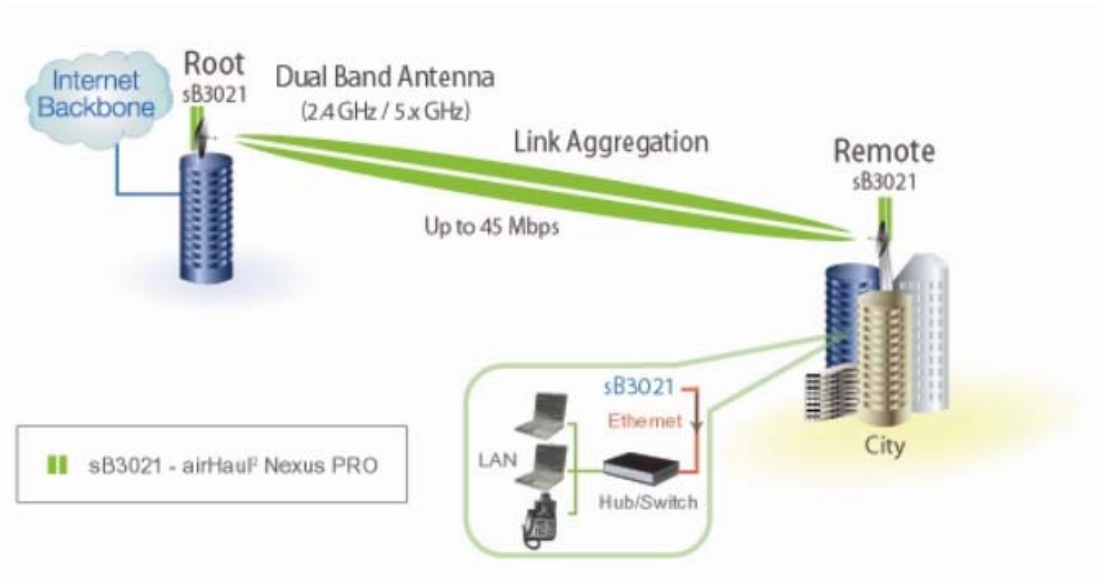


Figure 2-11 Link Aggregate Mode

As we can see from the above figure, both the radios in airHaul^2 Nexus PRO is configured in Link Aggregate mode to bridge the distance from Internet backbone to an office building to provide last mile connectivity. They are able to provide a higher bandwidth, which cannot be achieved using single radio models.

In this mode, the user needs to ensure that the Remote Device is configured as Link Aggregate Remote Router/NAT mode.

To configure the device in Link Aggregate Root Router Mode, follow these steps:

1. Go to Tools | System configuration drop down menu. The **System Configuration** will be displayed as shown below.

2. Click on the **Device Mode** link in the **System Configuration** page.

3. Choose the **Link Aggregate Root Router Mode** option and click on **Apply Changes**. A confirmation Wireless IP pop up window will appear as shown below.

4. After setting the wireless IP, click on **Apply Changes**. Please wait for the device to configure the settings in the Link Aggregate Root Router Mode. Radio A and Radio B will now be in Root Router Mode

5. **Both Radio A and Radio B need to be associated with the respective Radio A and Radio B of the Remote Device, which should be configured in Link Aggregate Remote Router/NAT Mode.**

   Note: Ensure that both local and remote devices are enabled for Link Aggregate Mode.

Note: When using Link Aggregate Root Router Mode, the Remote device should be configured in Link Aggregate Remote Router/NAT mode.

When Configuring the IP address for Link Aggregate Root Router and Link Aggregate Remote Router/NAT, you are required to assign the IP statically on both Root and Remote sides.

The Wireless IP address on the Root and Remote devices needs to be **3 host addresses apart**. The subnet mask cannot be less than 255.255.255.248.

For Example:

Root Router is configured as: **192.168.1.208** (The following sequence **192.168.1.209** and **192.168.1.210** cannot be assigned to any other hosts)

Netmask: **255.255.255.0**

Remote Router/NAT needs to be configured as: **192.168.1.211** (The following sequence **192.168.1.212** and **192.168.1.213** cannot be assigned to any other hosts)

Netmask : **255.255.255.0**

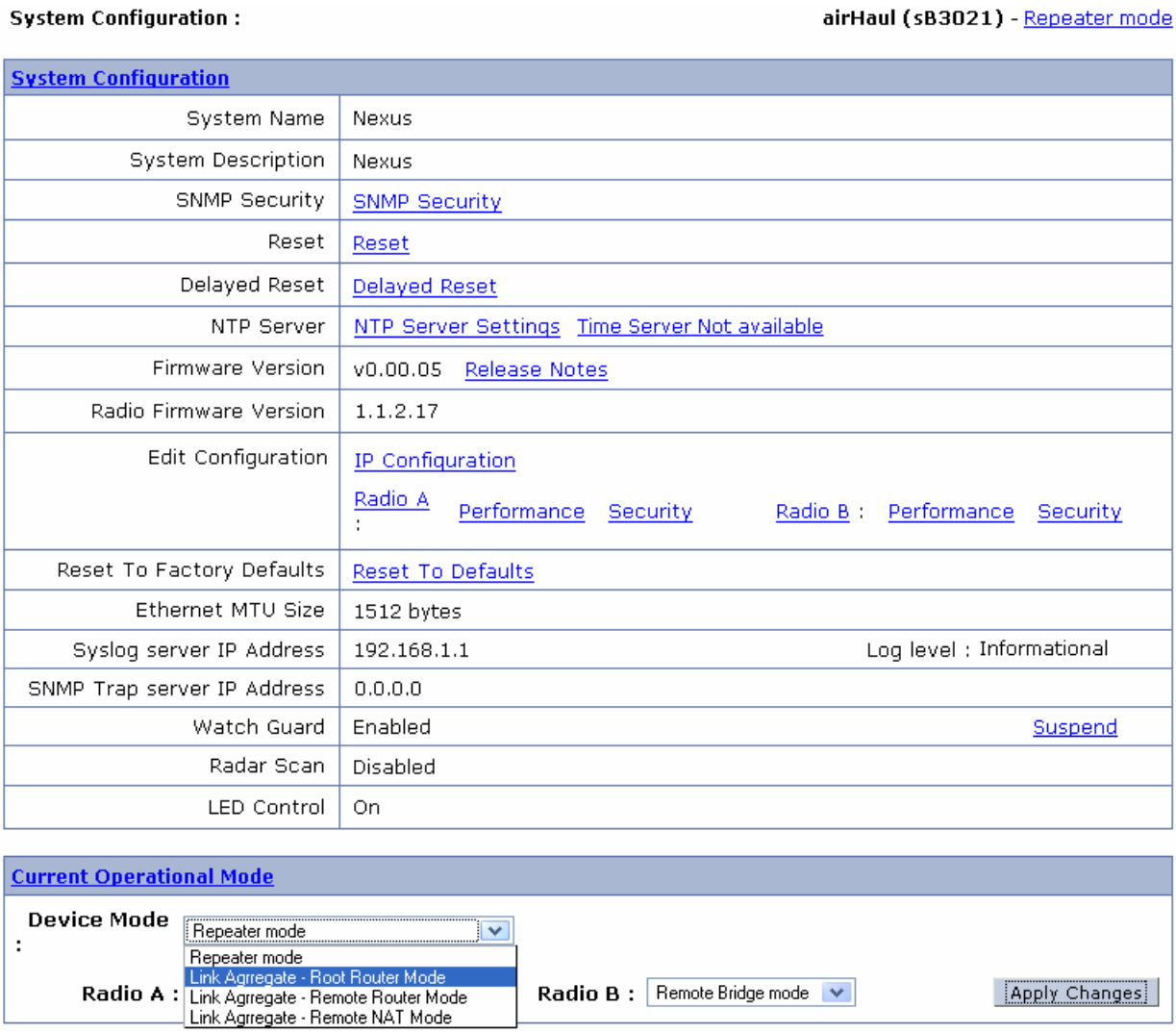


Figure 2-12 Link Aggregate Root Router Mode Configurations

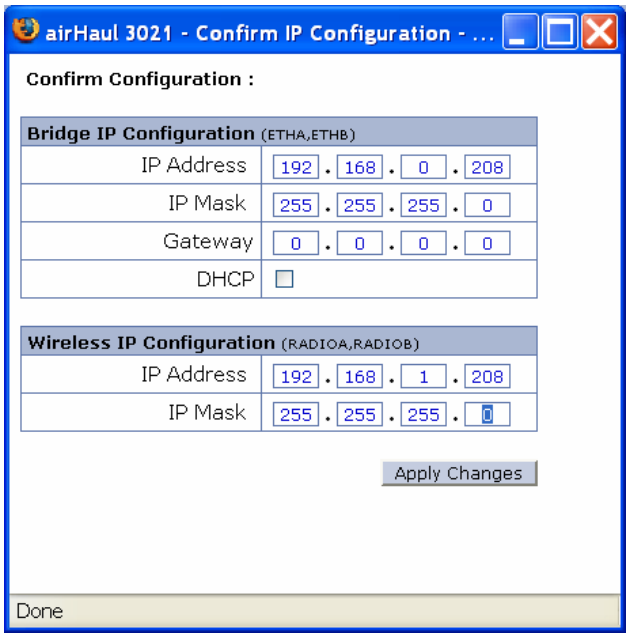

airHaul 3021 - Confirm IP Configuration - ...
Confirm Configuration :
Bridge IP Configuration (ETHA,ETHB)
IP Address 192 . 168 . 0 . 208
IP Mask 255 . 255 . 255 . 0
Gateway 0 . 0 . 0 . 0
DHCP
Wireless IP Configuration (RADIOA,RADIOB)
IP Address 192 . 168 . 1 . 208
IP Mask 255 . 255 . 255 .
Apply Changes
Done

Figure 2-13 Confirmation Wireless IP Configuration pop up window

After configuring the device as Link Aggregation Root Router mode, the summary page looks as follows:

Summary Information :

airHaul (sB3021) - Link Aggregate - Root Router Mode

Bridge IP Configuration (ETH A,ETH B)	
IP Address	192.168.0.208
IP Mask	255.255.255.0
Gateway	0.0.0.0
DHCP	Disabled

Wireless IP Configuration (RADIO A,RADIO B)	
IP Address	192.168.1.208
IP Mask	255.255.255.0

Radio A: Wireless Configuration	
SSID	DUT A
Channel	161 - (5805 MHz)
RSSI (dBm)	-45
Maximum Wireless Throughput (Kbps)	30720
Mode	Root Router

Radio B: Wireless Configuration	
SSID	DUT B
Channel	149 - (5745 MHz)
RSSI (dBm)	-51
Maximum Wireless Throughput (Kbps)	30720
Mode	Root Router

Port Information			
ETH A MAC Address	00:30:1A:1C:3D:9F	Radio A MAC Address	00:30:1A:1F:4C:62
ETH B MAC Address	00:30:1A:1C:3D:A0	Radio B MAC Address	00:30:1A:1F:49:73

Figure 2-14 Link Aggregate Root Router Mode (both radios are associated)

2.5.3 Link Aggregate Remote Router/NAT Mode

Follow the steps below for configuring the device in Link Aggregate Remote NAT Mode:

1. Go to Tools | System Configuration drop down Menu. The **System Configuration** will be displayed as shown below.
2. Click on the **Device Mode** link in the **System Configuration** page.
3. Choose **Link Aggregate Remote Router/NAT** option and click on **Apply Changes.** A confirmation Wireless IP pop up window will appear as shown below.
4. After setting the wireless IP, click on the '**Apply Changes**'. Refer to the figure below for the confirmation pop up window.

   Note: Please look into the **Example** in the 2.5.2 section, while configuring the Wireless IP for the Remote Router/NAT
5. Please wait for the device to configure the settings in the Link Aggregate Remote Router/NAT Mode. Radio A and Radio B will now be in Remote Router/NAT Mode.
6. Both Radio A and Radio B need to be associated with the respective Radio A and Radio B of the Root device which is configured in Link Aggregate Root Router Mode.

   Note: Ensure that both the radios are enabled for Link Aggregate Mode.

Note: Please look at the Radio Configuration Section for the Remote NAT Mode Configuration.

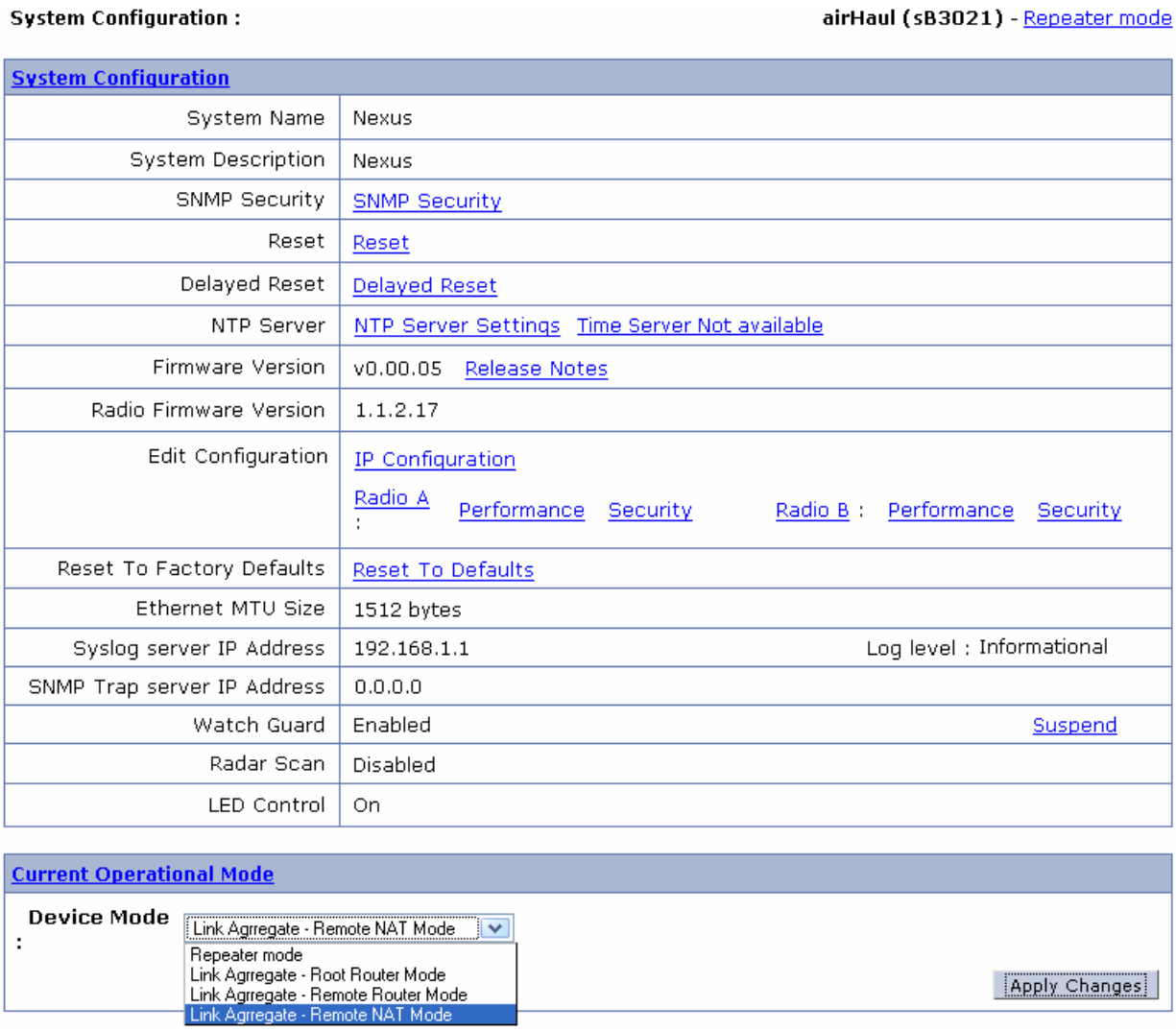


Figure 2-15 Link Aggregate – Remote Router/NAT Mode Configuration Page

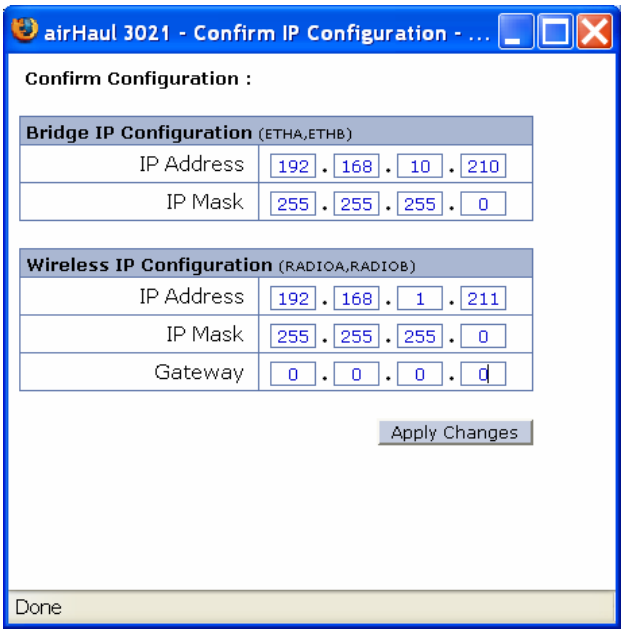

airHaul 3021 - Confirm IP Configuration - ...
Confirm Configuration :
Bridge IP Configuration (ETHA,ETHB)
IP Address 192 . 168 . 10 . 210
IP Mask 255 . 255 . 255 . 0
Wireless IP Configuration (RADIOA,RADIOB)
IP Address 192 . 168 . 1 . 211
IP Mask 255 . 255 . 255 . 0
Gateway 0 . 0 . 0 . 0
Apply Changes
Done

Figure 2-16 Confirmation Wireless IP pop up window

After configuring the device in Link Aggregation Remote NAT mode, the summary page looks as follows:

Summary Information : **airHaul (sB3021)** - Link Aggregate - Remote NAT Mode

Wireless IP Configuration (RADIO A, RADIO B)	
IP Address	192.168.10.208
IP Mask	255.255.255.0
Gateway	0.0.0.0

Bridge IP Configuration (ETH A,ETH B)	
IP Address	192.168.1.211
IP Mask	255.255.255.0

Radio A: Wireless Configuration	
SSID	DUT_A
Channel	7 - (2442 MHz)
Association Status	**Associated**
RSSI (dBm)	-53
Mode	Remote NAT

Radio B: Wireless Configuration	
SSID	DUT_B
Channel	112 - (5560 MHz)
Association Status	**Associated**
RSSI (dBm)	-62
Mode	Remote NAT

Port Information			
ETH A MAC Address	00:30:1A:16:20:6A	Radio A MAC Address	00:30:1A:28:F8:09
ETH B MAC Address	00:30:1A:16:20:6B	Radio B MAC Address	00:30:1A:28:F8:10

Figure 2-17 Link Aggregate – NAT Mode (both radios are associated)

2.6 Dual Radio Configuration

In the Repeater mode, the two radios in the airHaul^2 Nexus PRO are configured as Root and Remote. The configuration allows the user to configure the airHaul^2 Nexus PRO unit as Root Bridge, Remote Bridge or Remote Router/NAT mode.

By default, airHaul^2 Nexus PRO unit is set to Repeater Mode and one radio acts as Root Bridge and the other radio as Remote Bridge.

2.6.1 Root Bridge to Remote Bridge

Follow the steps below to change from Root Bridge mode to Remote Bridge mode:

1. Go to **Tools** | **System Configuration** drop down menu. The **System Configuration** will be displayed as shown below.
2. Alternatively, click on the **current device mode** link on the top right hand corner to go to the **System Configuration** page.
3. Click on the **Current Operational Mode**, select the radio that has to be configured as Remote Bridge and click on **Apply Changes**. A confirmation pop-up window will be displayed.
4. Enter IP Address, IP Mask and Gateway for **Ethernet Configuration**. DHCP is disabled by default and can be enabled if required.
5. Click on the **Apply Changes** button to change the settings. The device will reboot and be set to the chosen operational mode.

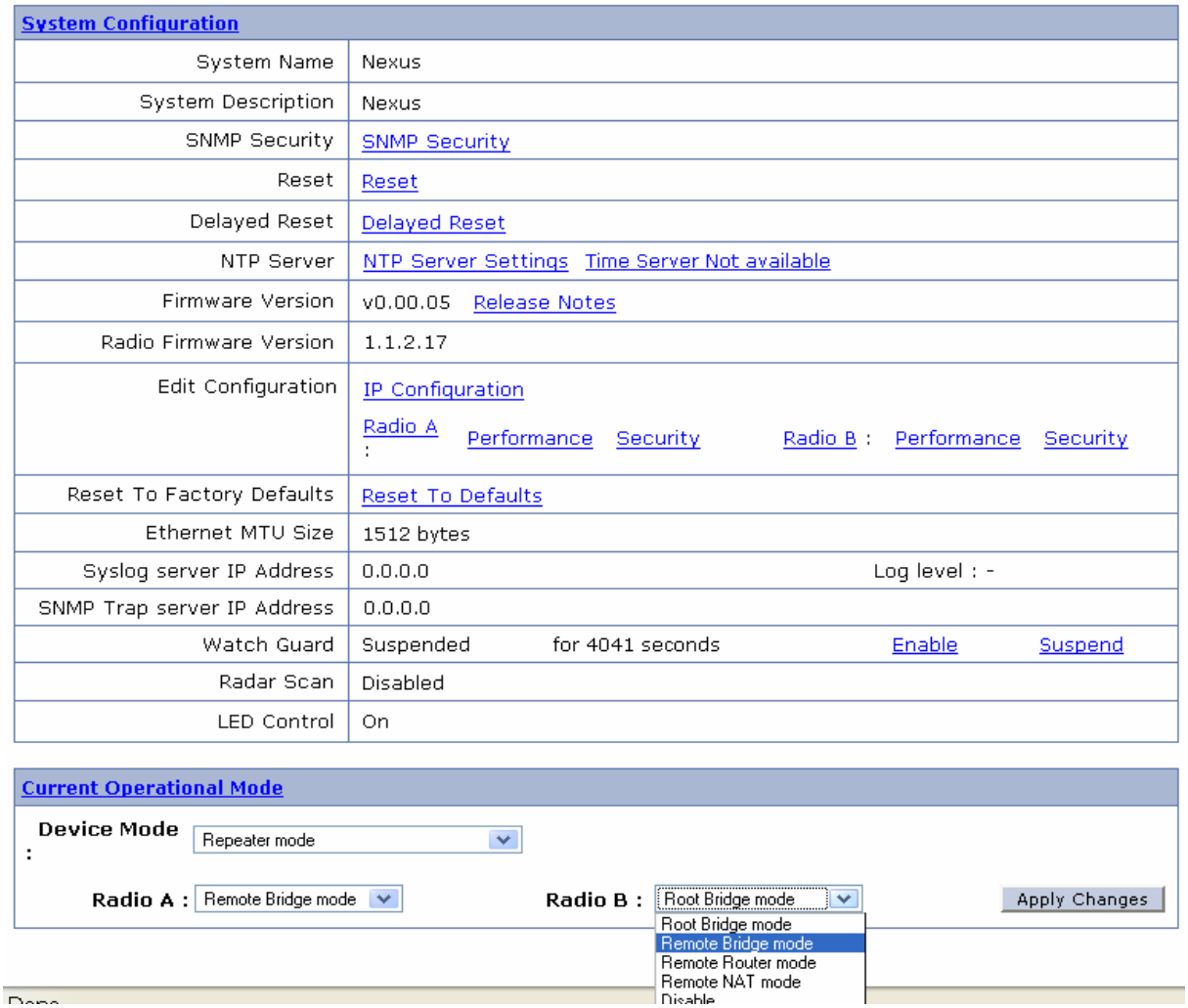


Figure 2-18 System Configuration Page – Root to Remote Bridge

Note: Before changing one of the radios to Remote, the other radio needs to be changed to Root Bridge first.

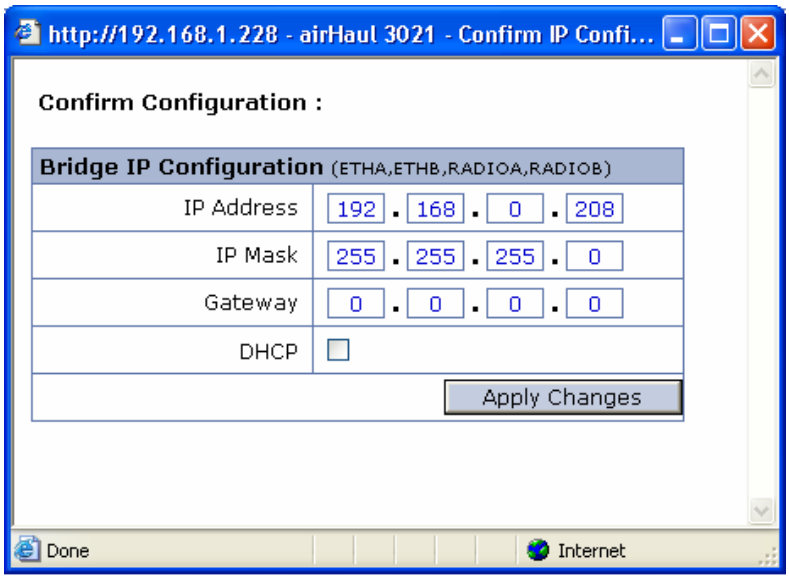


Figure 2-19 Changing Root Bridge to Remote Bridge

2.6.2 Root Bridge to Remote Router/NAT

Follow the steps below to change Root Bridge mode to Remote Router/NAT mode:

1 Go to **Tools** | **System Configuration** drop down menu. The **System Configuration** will be displayed as shown below.

2 Alternatively, click on the **Current Device Mode** link on the top right hand corner to go to the **System Configuration** page.

3 Click on the **Current Operational Mode** and select the radio that has to be configured as Remote Router/NAT. Click on **Apply Changes**. A confirmation pop-up window will be displayed.

4 Enter IP Address, IP Mask for **Ethernet Configuration,** the IP Address, IP Mask and Gateway for the wireless configuration. By default the DHCP is disabled and if required, it can be enabled.

5 Click on the **Apply Changes** button to change the settings. The device will be rebooted and set to the chosen operational mode.

Note: Before changing one radio to remote, the other radio needs to be changed to root bridge before doing a apply change.

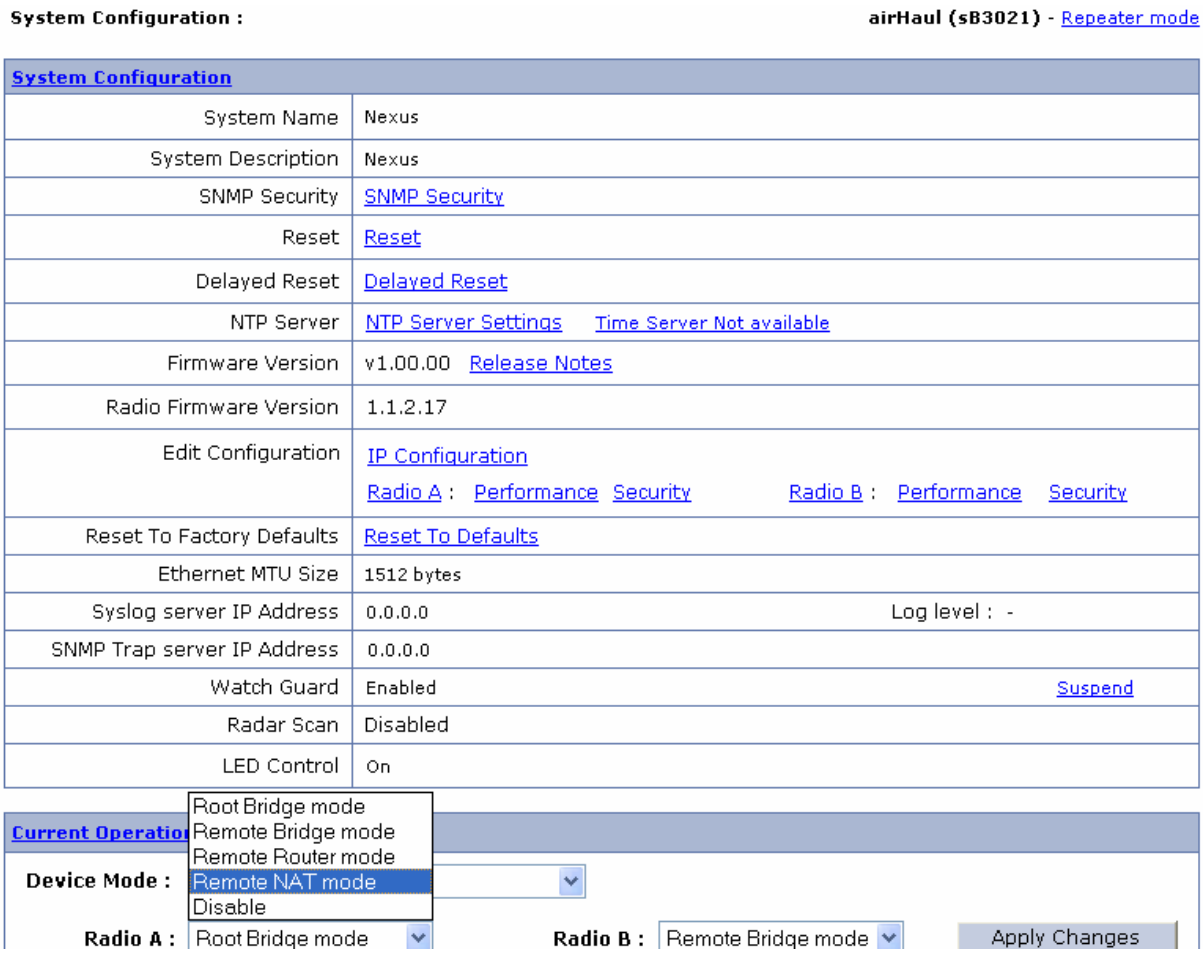


Figure 2-20 System Configuration Page – Root Bridge to Remote Router/NAT

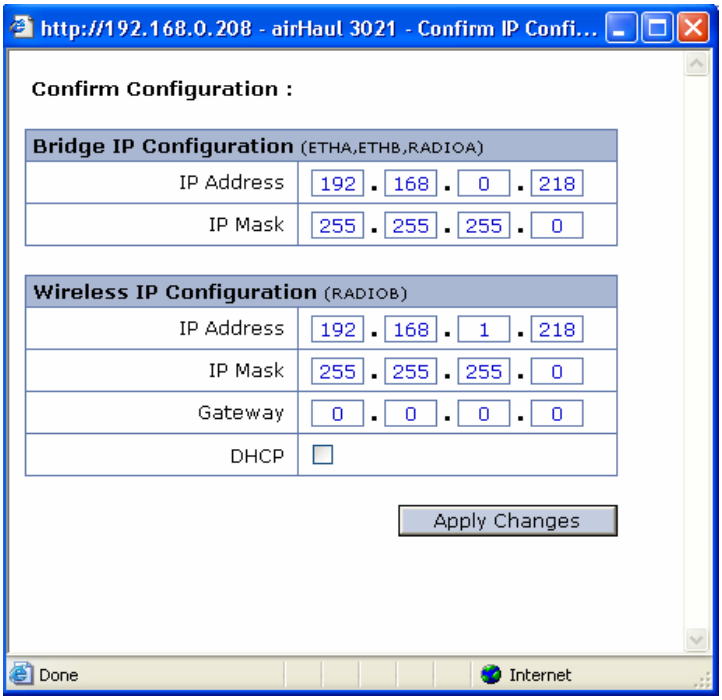

http://192.168.0.208 - airHaul 3021 - Confirm IP Confi...
Confirm Configuration :
Bridge IP Configuration (ETHA,ETHB,RADIOA)
IP Address 192 . 168 . 0 . 218
IP Mask 255 . 255 . 255 . 0
Wireless IP Configuration (RADIOB)
IP Address 192 . 168 . 1 . 218
IP Mask 255 . 255 . 255 . 0
Gateway 0 . 0 . 0 . 0
DHCP
Apply Changes
Done
Internet

Figure 2-21 Changing Root Bridge to Remote Router/NAT

2.6.3 Remote Bridge to Root Bridge

Follow the steps below to change Remote Bridge mode to Root Bridge mode:

1 Go to **Tools** | **System Configuration** drop down menu. The **System Configuration** will be displayed as shown below.

2 Alternatively, click on the **current device mode** link on the top right hand corner to go to the **System Configuration** page. .

3 Click on the "**Current Operational Mode**", Select the Radio that has to be configured as Root Bridge and click on **Apply Changes**. A confirmation pop-up window will be displayed.

4 Enter IP Address, IP Mask and Gateway for **Ethernet Configuration**. DHCP is disabled by default and can be enabled if required.

5 Click on the **Apply Changes** button to change the settings. The device will be rebooted and set to the chosen operational mode.

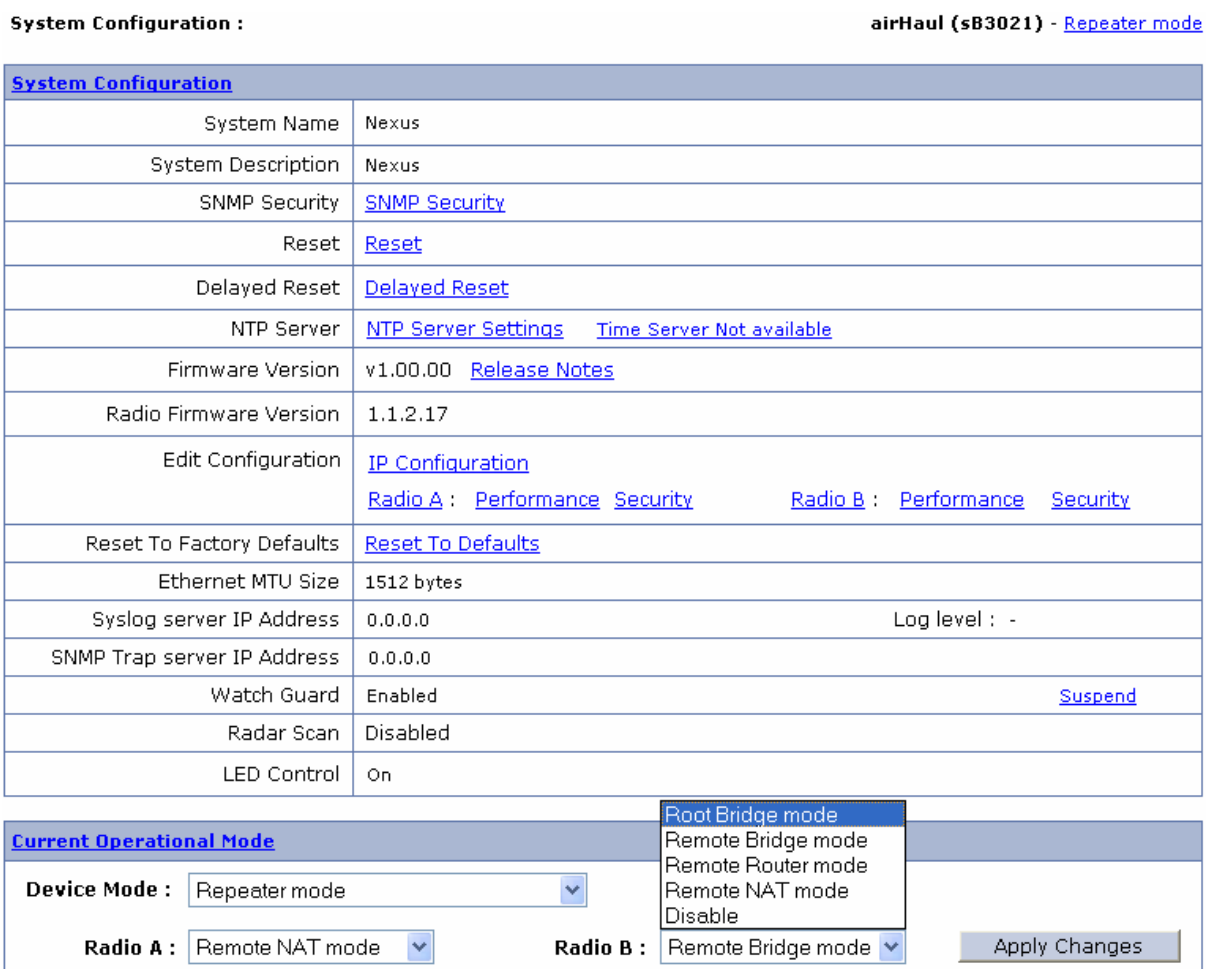


Figure 2-22 System Configuration--Remote Bridge to Root Bridge

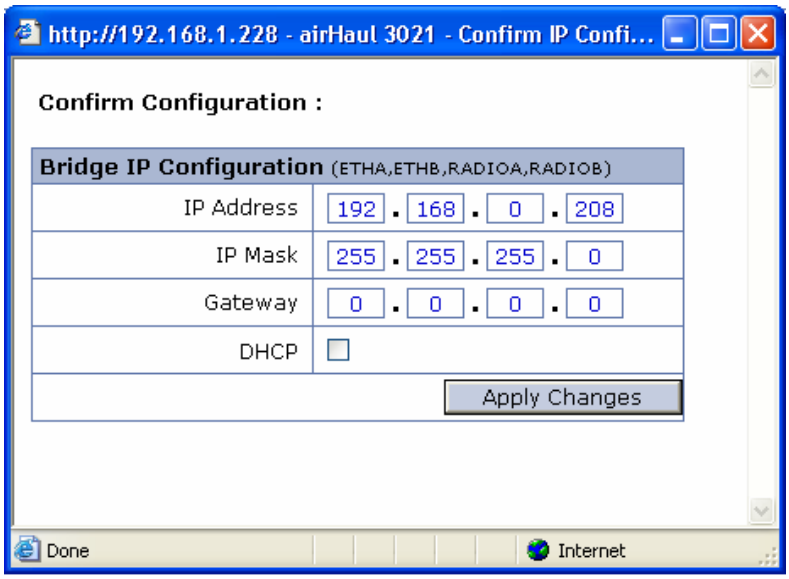


Figure 2-23 Changing Remote Bridge to Root Bridge

2.6.4 Remote Router/NAT to Root Bridge

Follow the steps below to change Remote Router/NAT mode to Root Bridge mode:

1 Go to **Tools** | **System Configuration** drop down menu. The **System Configuration** will be displayed as shown below.

2 Alternatively, click on the **current device mode** link on the top right hand corner to go to the **System Configuration** page. .

3 Click on the "**Current Operational Mode**", Select the Radio that has to be configured as Root Bridge and click on **Apply Changes**. A confirmation pop-up window will be displayed.

4 Enter the IP Address, IP Mask and Gateway for **Ethernet Configuration**. DHCP is disabled by default and can be enabled if required.

5 Click on the **Apply Changes** button to change the settings. The device will be rebooted and set to the chosen operational mode.

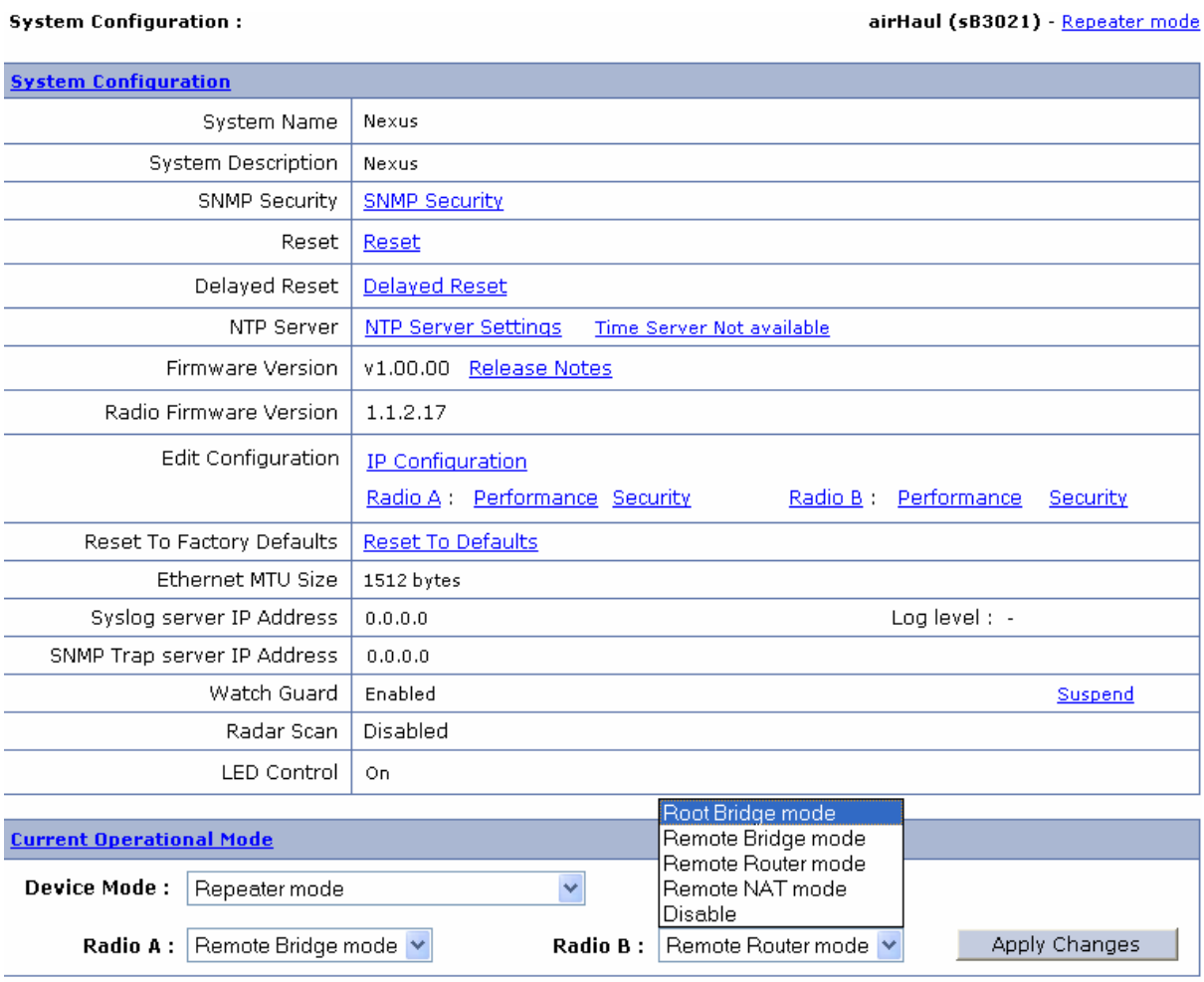


Figure 2-24 System Configuration Page--Remote Router/NAT to Root Bridge

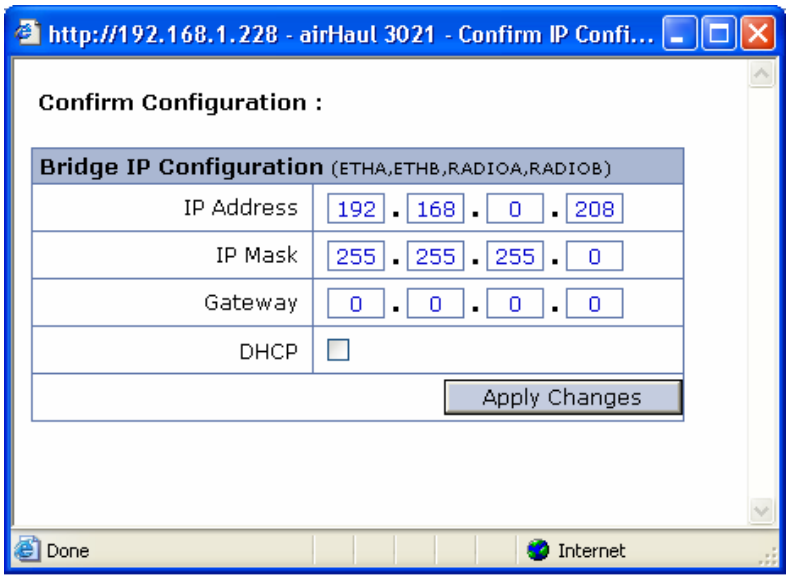


Figure 2-25 Changing Remote Router/NAT to Root Bridge

2.6.5 Remote Router/NAT to Remote Bridge

Follow the steps below to change Remote Router/NAT mode to Remote Bridge Mode:

1 Go to **Tools** | **System Configuration** drop down menu. The **System Configuration** will be displayed as shown below.

2 Alternatively, click on the **current device mode** link on the top right hand corner to go to the **System Configuration** page.

3 Click on "**Current Operational Mode"**, select the radio that has to be configured as Remote Bridge and click on **Apply Changes**. A confirmation pop-up window will be displayed.

4 Enter IP Address, IP Mask and Gateway for **Ethernet Configuration**. DHCP is disabled by default and can be enabled if required.

5 Click on the **Apply Changes** button to change the settings. The device will be rebooted and set to the chosen operational mode.

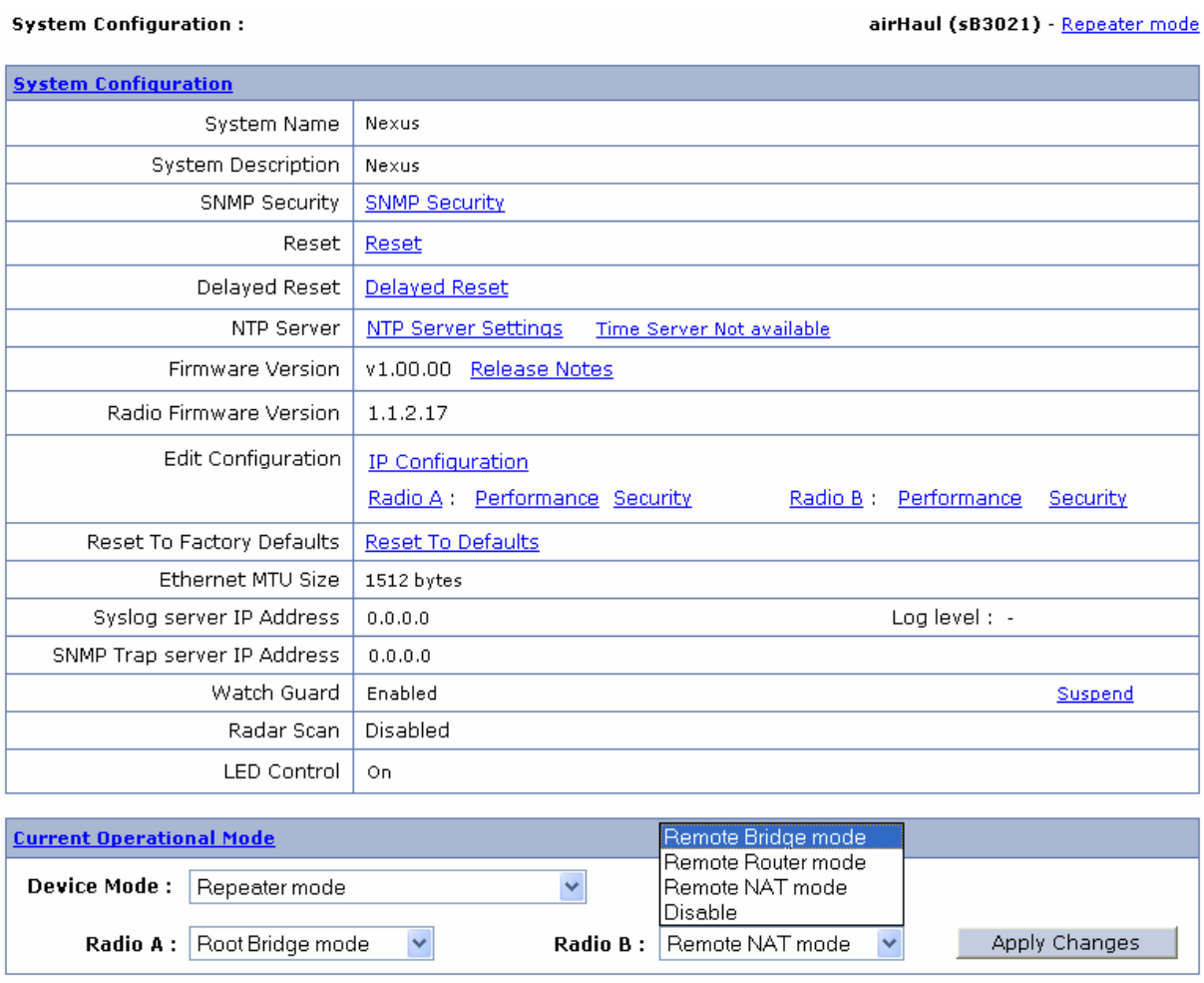


Figure 2-26 System Configuration Page--Remote Router/NAT to Remote Bridge

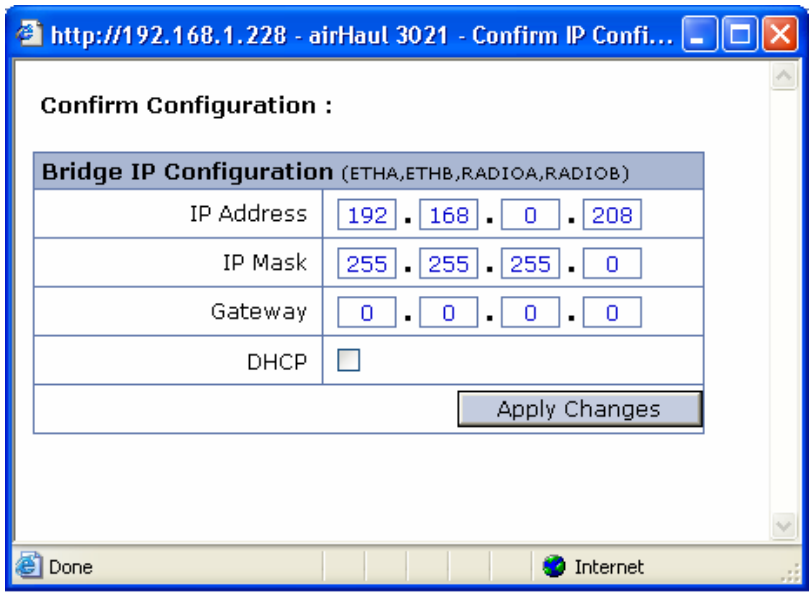


Figure 2-27 Changing Remote Router/NAT to Remote Bridge

2.6.6 Remote Bridge to Remote Router/NAT

Follow the steps below to change Remote Bridge mode to Remote Router/NAT mode

1 Go to **Tools** | **System Configuration** drop down menu. The **System Configuration** will be displayed as shown below.

2 Alternatively, click on the **current device mode** link on the top right hand corner to go to the **System Configuration** page.

3 Click on "**Current Operational Mode"**, Select the Radio that has to be configured as Remote Router/NAT and click on **Apply Changes**. A confirmation pop-up window will be displayed.

4 Enter IP Address, IP Mask for **Ethernet Configuration,** and the IP Address, IP Mask and Gateway for the Wireless configuration. By default the DHCP is disabled and can be enabled if required.

5 Click on the **Apply Changes** button to change the settings. The device will be rebooted and set to the chosen operational mode.

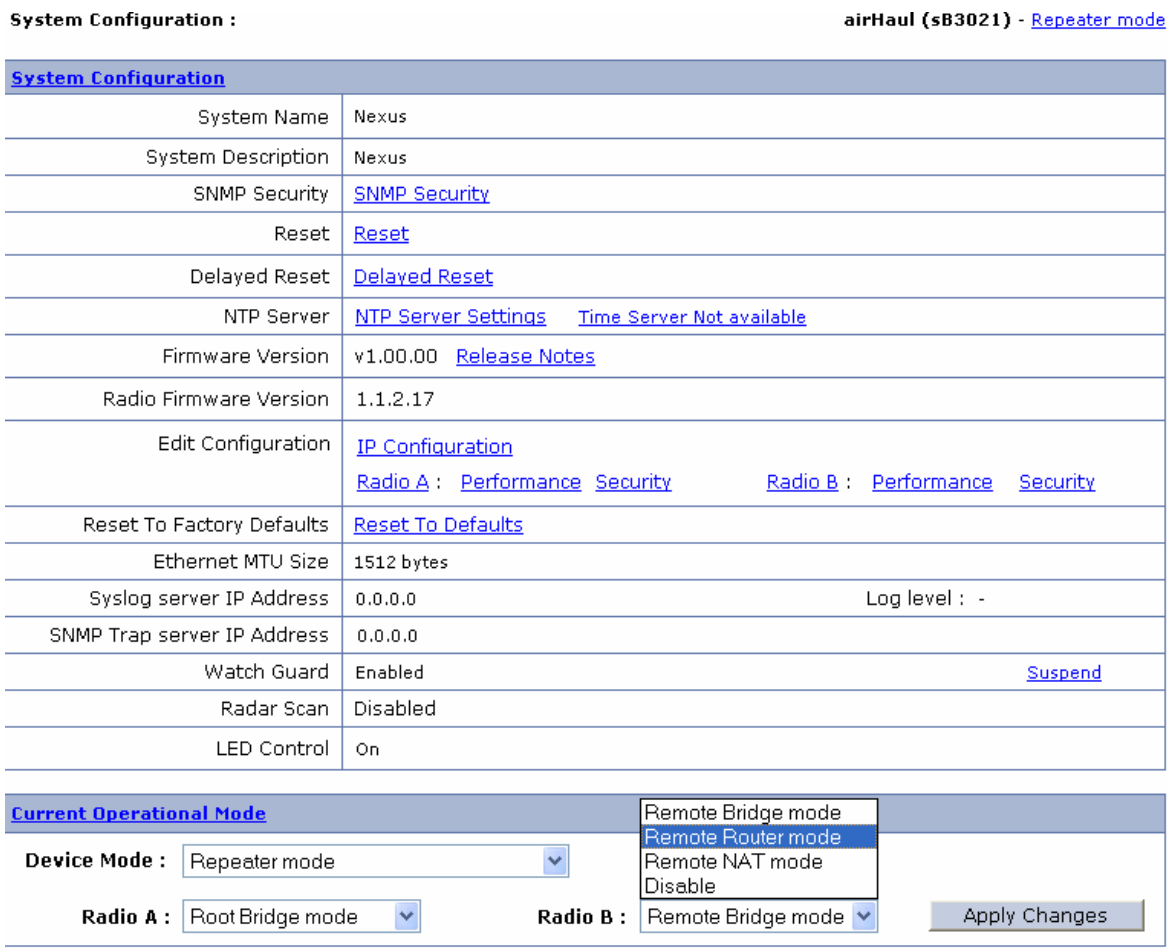


Figure 2-28: System Configuration page--Remote Bridge to Remote Router/NAT

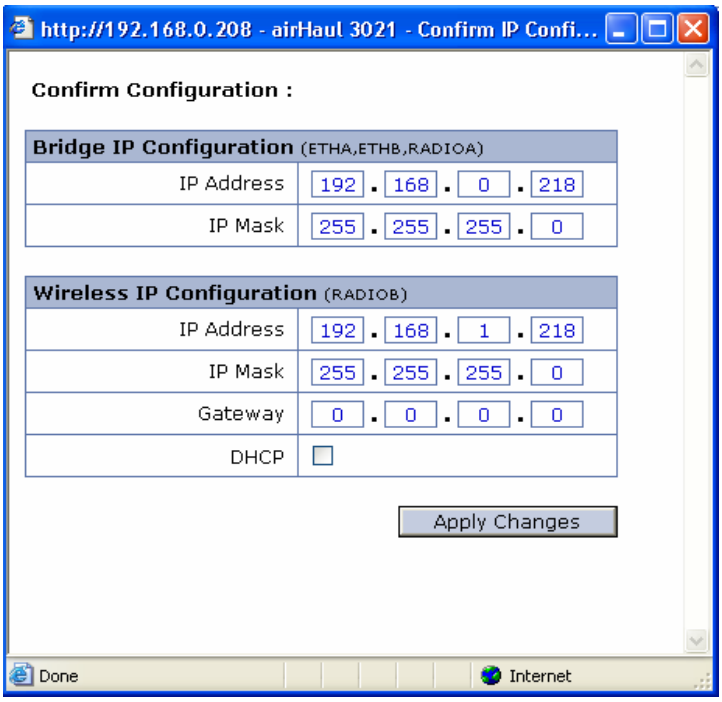

http://192.168.0.208 - airHaul 3021 - Confirm IP Confi...
Confirm Configuration :
Bridge IP Configuration (ETHA,ETHB,RADIOA)
IP Address 192 . 168 . 0 . 218
IP Mask 255 . 255 . 255 . 0
Wireless IP Configuration (RADIOB)
IP Address 192 . 168 . 1 . 218
IP Mask 255 . 255 . 255 . 0
Gateway 0 . 0 . 0 . 0
DHCP
Apply Changes
Done
Internet

Figure 2-29 Changing Remote Bridge to Remote Router/NAT

2.7 Root Bridge Configuration

The airHaul^2 Nexus PRO unit is configured in Root Bridge mode for use as a Root device. This section provides information on configuring in this mode.

2.7.1 Bridge IP Configurations

The Ethernet (wired-side) parameters need to be configured for the Root Bridge device to communicate with the wired LAN network. The airHaul^2 Nexus PRO unit supports two Ethernet ports function as a bridge. The Bridge IP Configuration provides configuration for the bridge IP parameters.

Follow the steps below to change the Root Bridge Ethernet Configurations:

1. From the **Summary Information** page, click on the **Bridge IP Configuration** link.
2. Enter a new **IP Address**, **IP Mask**, **Gateway** and **DHCP** status (check if it is enabled, otherwise uncheck to disable it). If DHCP is checked, the IP address will be assigned by the DHCP server in the network. If there is no DHCP server, the device will revert to the previous IP address after 60 seconds.
3. Click on the **Apply Changes** button to change the settings.

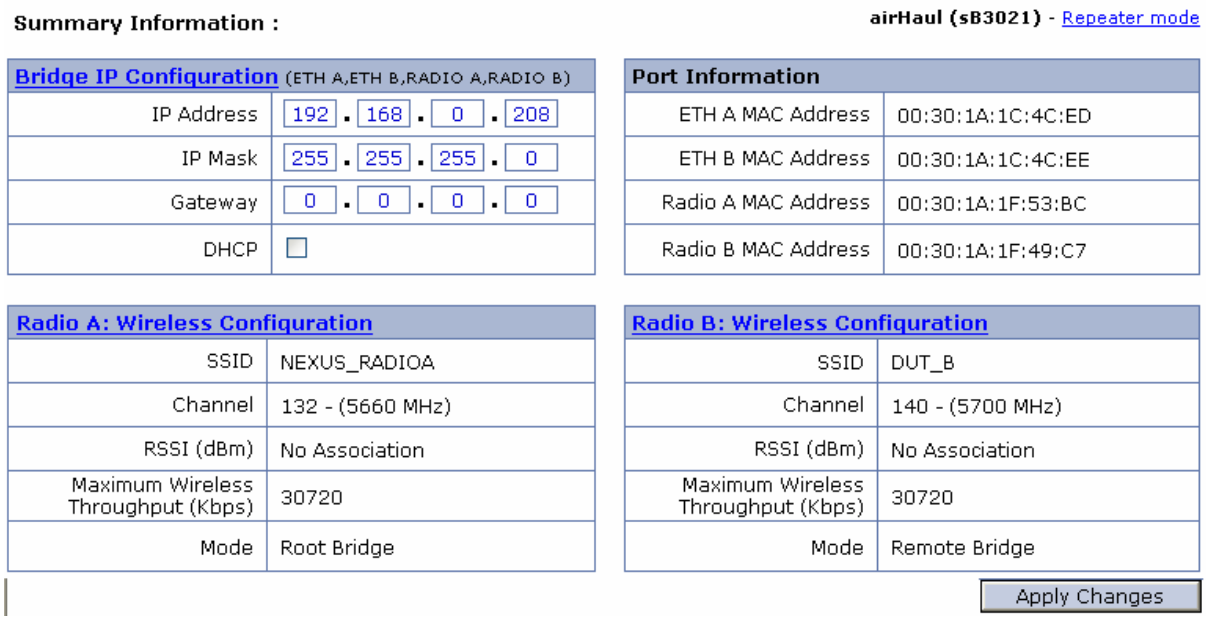

Summary Information :
airHaul (sB3021) - Repeater mode
Bridge IP Configuration (ETH A,ETH B,RADIO A,RADIO B)
IP Address 192 . 168 . 0 . 208
IP Mask 255 . 255 . 255 . 0
Gateway 0 . 0 . 0 . 0
DHCP
Port Information
ETH A MAC Address 00:30:1A:1C:4C:ED
ETH B MAC Address 00:30:1A:1C:4C:EE
Radio A MAC Address 00:30:1A:1F:53:BC
Radio B MAC Address 00:30:1A:1F:49:C7
Radio A: Wireless Configuration
SSID NEXUS_RADIOA
Channel 132 - (5660 MHz)
RSSI (dBm) No Association
Maximum Wireless Throughput (Kbps) 30720
Mode Root Bridge
Radio B: Wireless Configuration
SSID DUT_B
Channel 140 - (5700 MHz)
RSSI (dBm) No Association
Maximum Wireless Throughput (Kbps) 30720
Mode Remote Bridge
Apply Changes

Figure 2-30 Root Bridge Ethernet Configurations

2.7.2 Wireless Configurations

The wireless parameters need to be configured for the Root Bridge device to communicate with other airHaul^2 Nexus PRO Remotes.

Follow the steps below to change the Root Bridge Wireless Configurations:

1. From the **Summary Information** page, click on the **Wireless IP Configuration** link of the Radio that needs to be configured as Root Bridge, or go to menu bar and from the **Radio** dropdown menu select the particular radio that needs to be configured with the wireless settings in the Root Bridge Mode.
2. The **Radio Configuration** page will appear. Click on the **Wireless Settings** link.
3. Enter the **SSID** of the unit and select whether the **SSID Broadcast** has to **Enabled/Disabled**.
4. Select the Domain and the Channel.
5. Select the Transmit power of the radio from **Dial-a-Power** dropdown menu.
6. Select the gain of the antenna from the dropdown menu according to the gain of the antenna being used with the equipment.
7. Enter the RF cable loss based on the cable specifications.
8. Click on the **Apply Changes** button to change the settings.

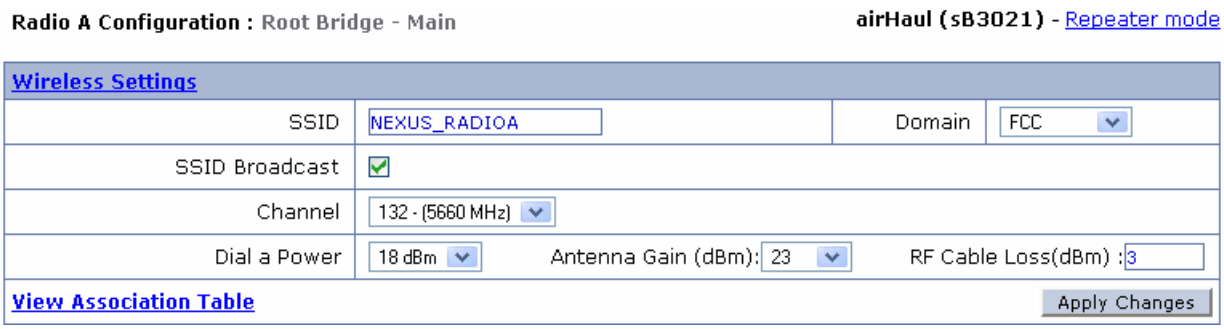


Figure 2-31 Root Bridge Wireless Settings

The following table summarizes the information for the wireless settings.

Table 2-3 Wireless Settings

Page Items	Descriptions
SSID	This is the current SSID. The user can change the SSID. The SSID is a unique identifier that wireless networking devices use to establish and maintain wireless connectivity. It is case sensitive and can contain up to 32 alphanumeric characters. Do not include special characters in the SSID.
Domain	This is the current radio regulatory domain. The user can choose the appropriate domain. The dropdown menu shows a list of domains supported by the radio. Different domains will show different channel lists.
Channel	This is the current radio channel in the selected domain. The user can choose other channels from the dropdown list. For a more consistent performance after a site survey, we recommend that the user select a non-overlapping channel setting for the radio. The radio channel settings correspond to the frequencies available in the user regulatory domain. **Note**: There should be a minimum separation of 40MHZ between the two radio channels.
Dial-a-Power	Dial-a-Power is used to set the output power of the radio at the N Connector. The valid radio power range is from -5 dBm to 23 dBm.
Antenna Gain	This is the gain of the antenna attached with the airHaul^2 Nexus PRO unit. The gain input here is merely for the purpose of display and for calculating the EIRP. The user can select anywhere between 2.2dBi to 30 dBi.
RF cable Loss	This refers to the loss of a cable connecting antenna to the airHaul^2 Nexus PRO unit
View Association Table	Lists all associated clients and its link status.

Note: The default value for Dial-a-Power is 18 dBm for FCC domain.
At high TX power levels, the radio tends to distort EVM due to the amplifier saturation and this affects throughput. If that happens, use a value lower than the maximum power level value, especially in the 5 GHz band.

Note: The default security of Root Bridge Mode is ACL+WEP so any WDS client or normal client needs to be added in the ACL either with WEP disabled/Enabled.

The figure below shows the list of clients associated with the airHaul^2 Nexus PRO Root Bridge device.

Figure 2-32 Root Bridge Association List

The MAC Address of the Link Status is the radio MAC of the associated remote device. The RSSI (Received Signal Strength Indication) is measured in dBm.

Click on the **Link Status** link to view the Link Status graph shown below.

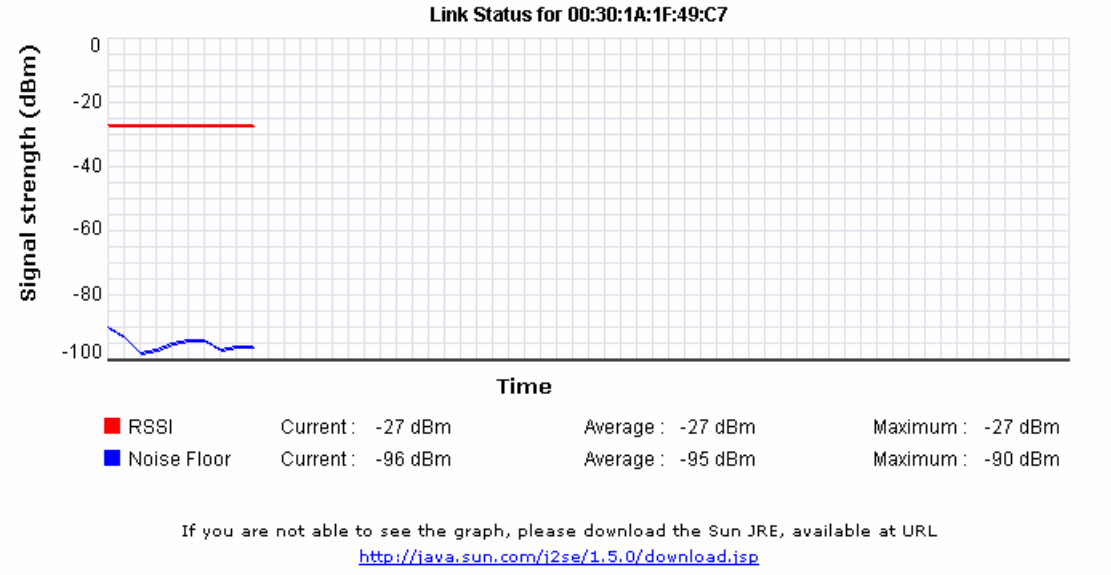
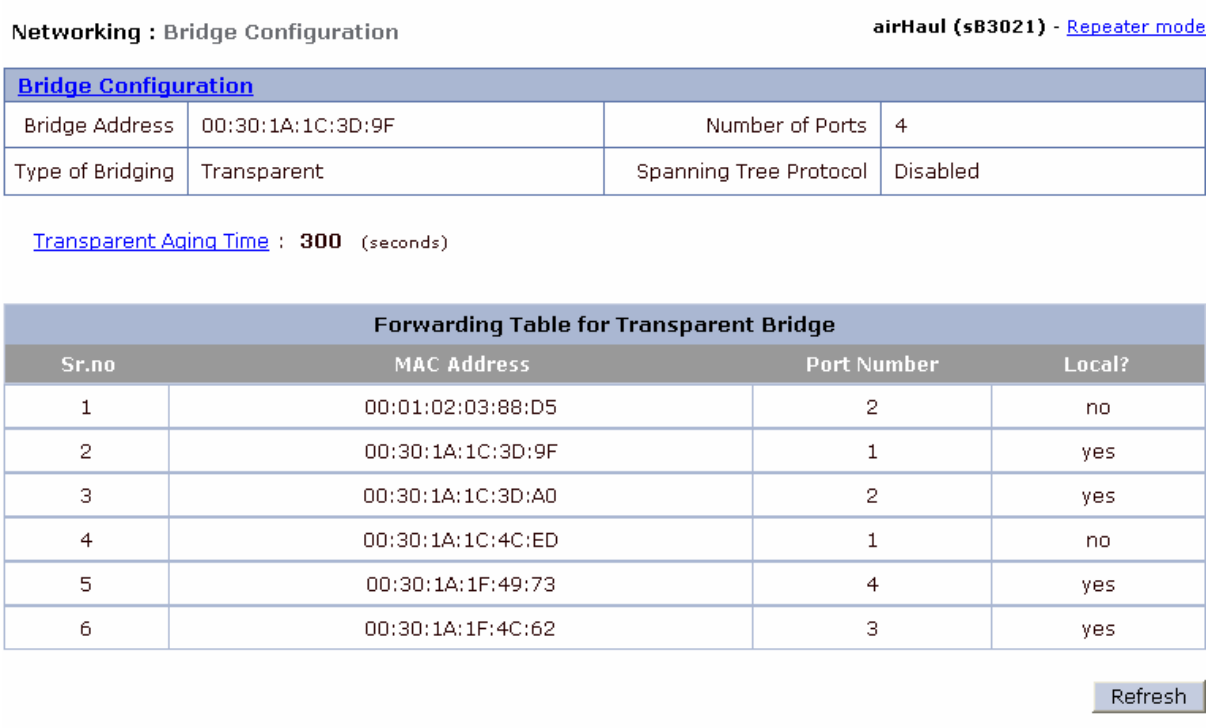

Link Status for 00:30:1A:1F:49:C7
Signal strength (dBm)
0
-20
-40
-60
-80
-100
Time
RSSI Current : -27 dBm Average : -27 dBm Maximum : -27 dBm
Noise Floor Current : -96 dBm Average : -95 dBm Maximum : -90 dBm
If you are not able to see the graph, please download the Sun JRE, available at URL
http://java.sun.com/j2se/1.5.0/download.jsp

Figure 2-33 Remote Link Status Bridge Configuration

In Bridge mode, the airHaul^2 Nexus PRO unit acts as a transparent bridge between the Radio and the Ethernet interfaces. The figure below shows the bridge configuration and the bridge forwarding table information. The STP (Spanning Tree Protocol) is disabled by default.



Networking : Bridge Configuration

airHaul (sB3021) - Repeater mode

Bridge Configuration			
Bridge Address	00:30:1A:1C:3D:9F	Number of Ports	4
Type of Bridging	Transparent	Spanning Tree Protocol	Disabled

Transparent Aging Time : 300 (seconds)

Forwarding Table for Transparent Bridge			
Sr.no	MAC Address	Port Number	Local?
1	00:01:02:03:88:D5	2	no
2	00:30:1A:1C:3D:9F	1	yes
3	00:30:1A:1C:3D:A0	2	yes
4	00:30:1A:1C:4C:ED	1	no
5	00:30:1A:1F:49:73	4	yes
6	00:30:1A:1F:4C:62	3	yes

Refresh

Figure 2-34 Bridge Configuration Information

2.7.3 Configuring Spanning Tree Protocol (STP)

STP is a Layer 2 link management protocol that provides path redundancy while preventing loops in the network. For a Layer 2 Ethernet network to function properly, only one active path can exist between any two redundant links.

To create a fault-tolerant network, there needs to be a loop-free path between all nodes in the network. The Spanning Tree Algorithm calculates the best loop-free path throughout a Layer 2 network. Infrastructure devices such as wireless bridges and switches send and receive spanning tree frames, called Bridge Protocol Data Units (BPDUs), at regular intervals. The devices do not forward these frames but use them to construct the loop-free path.

Multiple active paths among end stations cause loops in the network. If a loop exists in the network, end stations might receive duplicate messages. Infrastructure devices might also learn end-station MAC addresses on multiple Layer 2 interfaces. Such conditions result in an unstable network.

STP defines a tree with a root bridge and a loop-free path from the root to all infrastructure devices in the Layer 2 network.

STP forces redundant data paths into a standby (blocked) state. If a network segment in the spanning tree fails and a redundant path exists, the Spanning Tree Algorithm recalculates the spanning tree topology and activates the standby path.

When two interfaces on a device are part of a loop, the spanning tree port priority and path cost settings determine which interface is put in the forwarding state and which is put in the blocking state. The port priority value represents the location of an interface in the network topology and how well it is located to pass traffic. The path cost value represents the media speed.

2.7.4 STP Settings Configuration

STP is disabled by default. The table below lists the default STP settings when STP is enabled.

Table 2-4 Default STP Values

Setting	Default Value	Range	Purpose
Bridge priority	32768	0-65535	A parameter used to identify the root bridge in a spanning tree (instance of STP). The bridge with the lowest value has the highest priority and is the root.
Bridge max age	20	6-40	The interval a bridge will wait for a hello packet from the root bridge before initiating a topology change.
Bridge hello time	2	1-10	The interval of time between each configuration BPDU sent by the root bridge.

Bridge forward delay	15	4-30	The period of time a bridge will wait (the listen and learn period) before beginning to forward data packets.
Ethernet port (ETH A) path cost	100	0-65535	The cost of using the port to reach the root bridge. When selecting among multiple links to the root bridge, STP chooses the link with the lowest path cost and blocks the other paths. Each port type has its own default STP path cost.
Ethernet port (ETH A) priority	128	0-255	The preference that STP gives to this port relative to the other ports for forwarding traffic out of the spanning tree. A higher numerical value means a lower priority; thus, the highest priority is 8.
Ethernet port (ETH B) path cost	100	0-65535	The cost of using the port to reach the root bridge. When selecting among multiple links to the root bridge, STP chooses the link with the lowest path cost and blocks the other paths. Each port type has its own default STP path cost.
Ethernet port (ETH B) priority	128	0-255	The preference that STP gives to this port relative to the other ports for forwarding traffic out of the spanning tree. A higher numerical value means a lower priority; thus, the highest priority is 8.
Radio port (Radio A) path cost	100	0-65535	The cost of using the port to reach the root bridge. When selecting among multiple links to the root bridge, STP chooses the link with the lowest path cost and blocks the other paths. Each port type has its own default STP path cost.

Radio port (Radio A) priority	128	0-255	The preference that STP gives to this port relative to the other ports for forwarding traffic out of the spanning tree. A higher numerical value means a lower priority; thus, the highest priority is 8.

The Radio and Ethernet interfaces are assigned to bridge group by default. When the user enables STP and assigns a priority on bridge, STP is enabled on the radio and Ethernet interfaces. The interfaces adopt the priority assigned to bridge.
The user can edit the STP Priority, Bridge Max age, Bridge hello time, Forward Delay, STP Port priority and STP Port Path cost.

The **Transparent Aging Time** determines the time to refresh entries in the Forwarding Table. The Transparent Aging Time default value is **300** seconds.

Follow the steps below to configure the bridge STP in Root Bridge or Remote Bridge:

1. Click on **Networking** | **Bridge Configuration** to access the Bridge Configuration page.
2. Choose **Enable** from the Spanning Tree Protocol pull down list.
3. Click on the **Generic Bridge Port Table** link to change the Generic Parameters.
4. Enter a value for the **STP Priority**.
5. Enter values for the **Bridge Max Age**, **Bridge Hello Time** and **Bridge Forward Delay**
6. Click on **Transparent Aging Time** link to change the **Transparent Aging Time**.
7. Click on the **Spanning Tree Port Table** link to change the 'STP Ethernet Port' parameters.
8. Enter the values of Ethernet Port Priority and/or Port Path Cost for ETH A
9. Enter the values of Ethernet Port Priority and/or Port Path Cost for ETH B
10. Enter the values of Ethernet Port Priority and/or Port Path Cost for Radio A
11. Click on **Apply Changes** Button to save to the current configuration file.

Bridge Configuration			
Bridge Address	00:30:1A:1C:3A:E9	Number of Ports	3
Type of Bridging	Transparent	Spanning Tree Protocol	Enabled

Generic Bridge Port Table	
Protocol Specification	0
STP Priority	32768
Topology change Timer	0
STP designated Root	8000.00301a1c3ae9
STP Root Cost	0
STP Root Port	0
Bridge Max Age	20 (seconds)
Bridge Hello Time	2 (seconds)
Bridge Forward Delay	15 (seconds)

Spanning Tree Port Table			
	ETH A	ETH B	Radio A
Port	1	2	3
Port Priority	128	128	128
Port State	Forwarding	Forwarding	Forwarding
Port Enable	Yes	Yes	Yes
Port Path Cost	100	100	100
Port Designated Root	8000. 00301a1c3ae9	8000. 00301a1c3ae9	8000. 00301a1c3ae9
Port Designated Cost	0	0	0
STP Designated Port	8001	8002	8003

Transparent Aging Time : **300** (seconds)

Forwarding Table for Transparent Bridge			
Sr.no	MAC Address	Port Number	Local?
1	00:30:1A:1F:49:A7	3	yes
2	00:30:1A:1C:3A:EA	2	yes
3	00:30:1A:1C:3A:E9	1	yes
4	00:30:1A:01:98:09	2	no

Figure 2-35 Bridge Configuration

2.8 Remote Bridge Configuration

The airHaul^2 Nexus PRO units can also be configured to operate as a Remote device to associate with a Root Bridge.

2.8.1 Bridge IP Configuration

The Ethernet IP is configured during the operational mode change to Remote Bridge mode.

Follow these steps below if you need to re-configure the Remote Bridge Ethernet parameters:

1. From the **Summary Information** page, click on the **Bridge IP Configuration** link to change Ethernet parameters.
2. Enable or disable the DHCP by clicking the check box. Enter the 'IP Address', 'IP mask', 'Gateway' for non DHCP. Assign the unit a unique IP Address with the same IP subnet (e.g. 192.168.0.100) as the Root device it will be associated to.
3. Click on the '**Apply Changes'** button to change the settings.

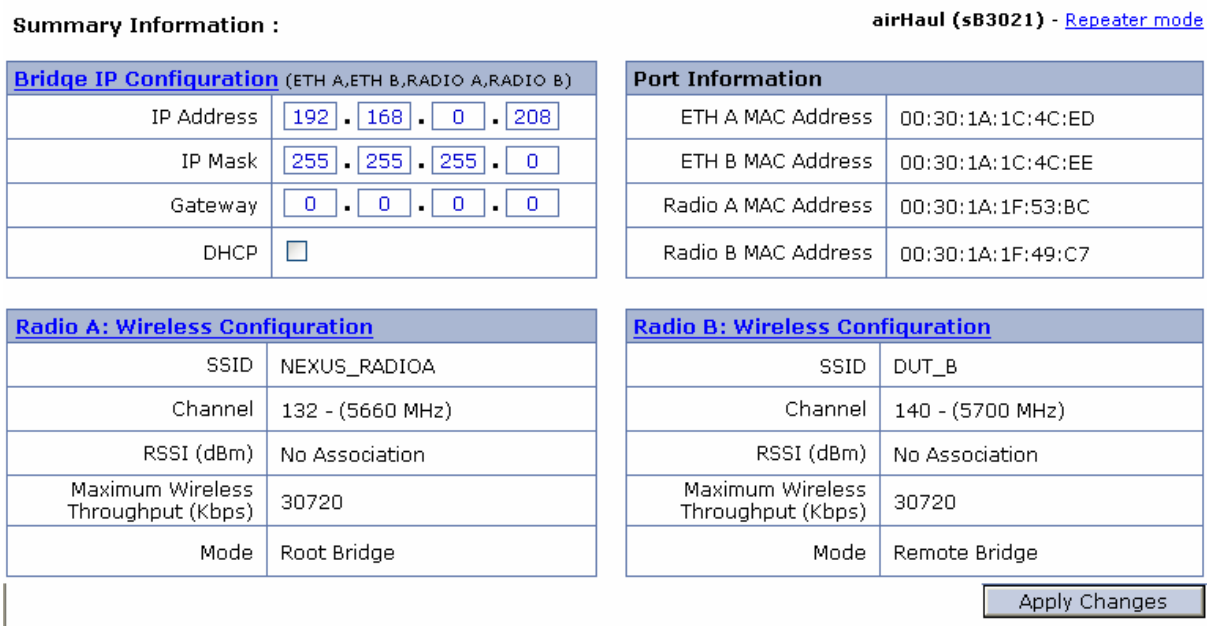

Summary Information :
airHaul (sB3021) - Repeater mode
Bridge IP Configuration (ETH A,ETH B,RADIO A,RADIO B)
IP Address 192 . 168 . 0 . 208
IP Mask 255 . 255 . 255 . 0
Gateway 0 . 0 . 0 . 0
DHCP
Port Information
ETH A MAC Address 00:30:1A:1C:4C:ED
ETH B MAC Address 00:30:1A:1C:4C:EE
Radio A MAC Address 00:30:1A:1F:53:BC
Radio B MAC Address 00:30:1A:1F:49:C7
Radio A: Wireless Configuration
SSID NEXUS_RADIOA
Channel 132 - (5660 MHz)
RSSI (dBm) No Association
Maximum Wireless Throughput (Kbps) 30720
Mode Root Bridge
Radio B: Wireless Configuration
SSID DUT_B
Channel 140 - (5700 MHz)
RSSI (dBm) No Association
Maximum Wireless Throughput (Kbps) 30720
Mode Remote Bridge
Apply Changes

Figure 2-36 Remote Bridge Ethernet Configuration

2.8.2 Wireless Configuration

The wireless parameters need to be configured to allow the Remote Bridge airHaul^2 Nexus PRO unit to associate with the Root Bridge unit.

Follow these steps below to configure the Remote Bridge Mode wireless association parameters:

1 Go to the menu bar and from the **Radio** dropdown menu, select the particular radio that has to be configured with the wireless settings in the Remote Bridge Mode.

2 Enter the SSID of the Root Bridge airHaul^2 Nexus PRO unit.

3 Enter the radio MAC address of the Root Bridge airHaul^2 Nexus PRO unit.

4 Choose a radio domain from the drop down list.

5 Choose a radio channel to associate the client with the root device.

6 Select the Transmit power of the radio from Dial-a-Power dropdown menu

7 Select the gain of the antenna from the dropdown menu as per the gain of the antenna being used with the equipment.

8 Enter the RF cable loss based on the cable specifications

9 Click the **Apply Changes**. The units will attempt to associate.

Note: Clicking on **'Status'** will display further details on the association

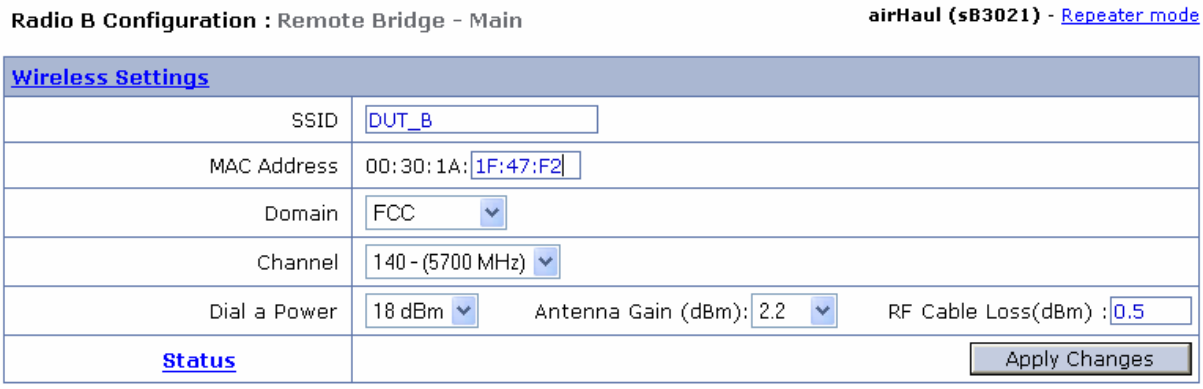


Figure 2-37 Remote Bridge Wireless Settings

Radio B Configuration : Remote Bridge - Main

airHaul (sB3021) - Repeater mode

Wireless Settings			
SSID	DUT_B **Associated**		
MAC Address	00:30:1A:1F:47:F3		
Domain	FCC		
Channel	140 - (5700 MHz)		
Dial a Power	18 dBm	Antenna Gain (dBm):2.2	RF Cable Loss(dBm) :0.5
Status			

Figure 2-38 Remote Bridge Associated

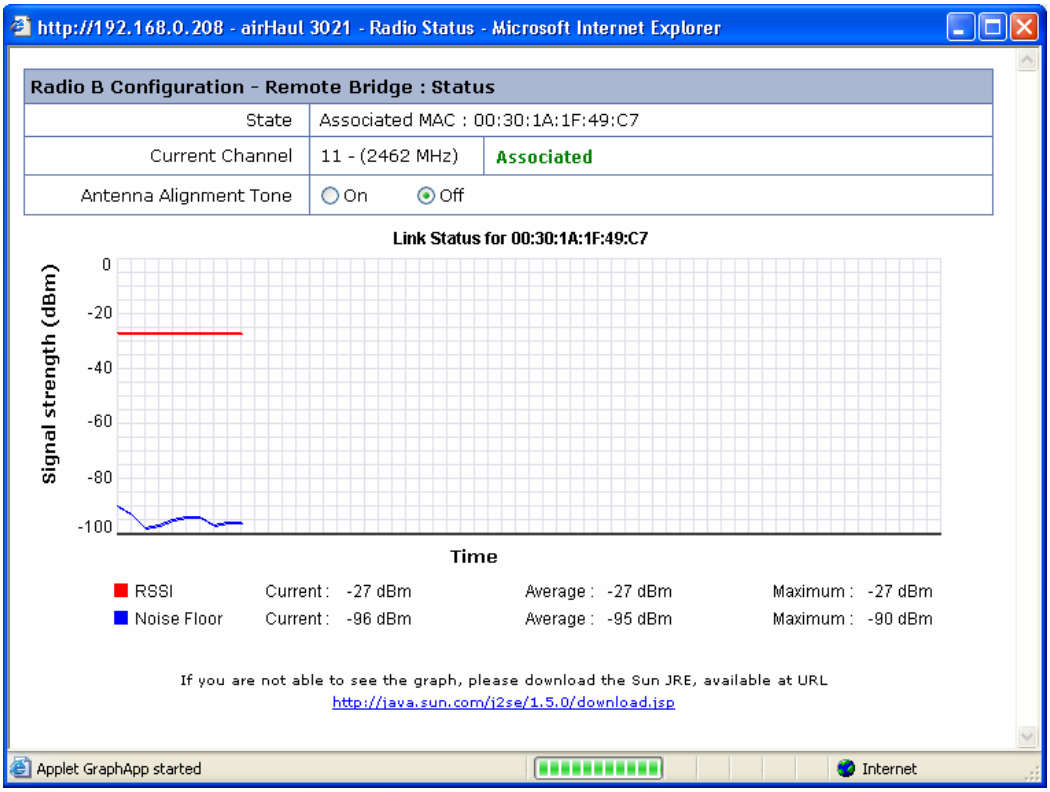


Figure 2-39 Remote Bridge Association with Root Bridge

If the association status window does not appear, click on the link to download the JRE.

Note: For Bridge and STP configuration, please refer to the section 2.6.3.

2.9 Remote Router/NAT Configuration

The airHaul^2 Nexus PRO units can also be configured to operate as a Remote device to associate with Root Bridge. In Remote Mode the unit can operate as Bridge or Router.

2.9.1 Bridge IP Configuration

The Ethernet IP is configured when the operational mode of one of the radios is configured as Remote Router/NAT.

Follow these steps below if you need to re-configure the Remote Router/NAT Ethernet parameters:

1. From the 'Summary Information' page, click on the '**Bridge IP Configuration**' link to change Ethernet parameters.
2. Enter the 'IP address' and 'IP mask'.
3. Click on the '**Apply Changes**' button to change the settings.

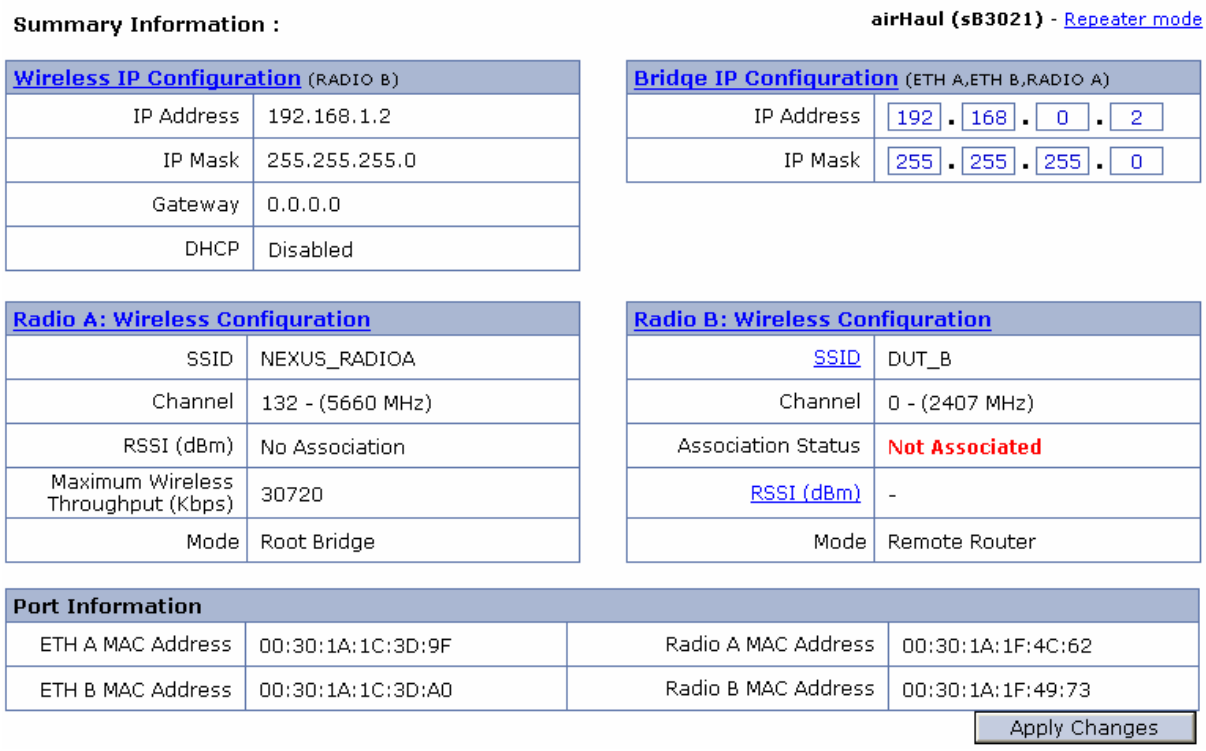

Summary Information :
airHaul (sB3021) - Repeater mode
Wireless IP Configuration (RADIO B)
IP Address 192.168.1.2
IP Mask 255.255.255.0
Gateway 0.0.0.0
DHCP Disabled
Bridge IP Configuration (ETH A,ETH B,RADIO A)
IP Address 192 . 168 . 0 . 2
IP Mask 255 . 255 . 255 . 0
Radio A: Wireless Configuration
SSID NEXUS_RADIOA
Channel 132 - (5660 MHz)
RSSI (dBm) No Association
Maximum Wireless Throughput (Kbps) 30720
Mode Root Bridge
Radio B: Wireless Configuration
SSID DUT_B
Channel 0 - (2407 MHz)
Association Status Not Associated
RSSI (dBm) -
Mode Remote Router
Port Information
ETH A MAC Address 00:30:1A:1C:3D:9F
Radio A MAC Address 00:30:1A:1F:4C:62
ETH B MAC Address 00:30:1A:1C:3D:A0
Radio B MAC Address 00:30:1A:1F:49:73
Apply Changes

Figure 2-40 Remote Router/NAT Ethernet Configurations

2.9.2 Wireless Configuration

The wireless parameters need to be configured to allow the Remote Router/NAT airHaul^2 Nexus PRO unit to associate with the Root Bridge unit.

Follow these steps below to configure the Remote Router/NAT Mode Wireless IP Settings parameters:

1. Click on the '**Wireless IP Configuration**' link from the 'Summary Information' page.
2. Enter the wireless 'IP address', 'IP Mask' and 'Gateway IP' address for the airHaul^2 Nexus PRO unit.
3. Check the 'Enable DHCP' checkbox to obtain an IP address automatically from network.
4. Click on the '**Apply Changes**' to change the settings.

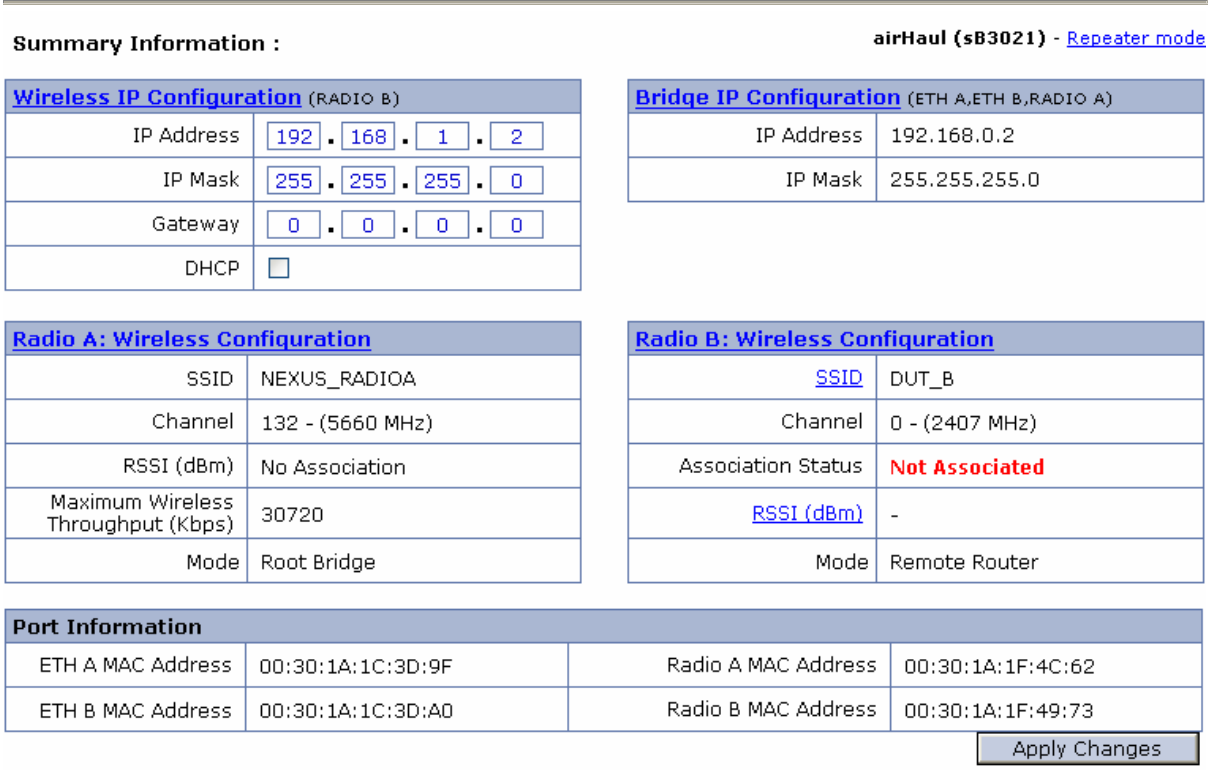

Summary Information :
airHaul (sB3021) - Repeater mode
Wireless IP Configuration (RADIO B)
IP Address 192 . 168 . 1 . 2
IP Mask 255 . 255 . 255 . 0
Gateway 0 . 0 . 0 . 0
DHCP
Bridge IP Configuration (ETH A,ETH B,RADIO A)
IP Address 192.168.0.2
IP Mask 255.255.255.0
Radio A: Wireless Configuration
SSID NEXUS_RADIOA
Channel 132 - (5660 MHz)
RSSI (dBm) No Association
Maximum Wireless Throughput (Kbps) 30720
Mode Root Bridge
Radio B: Wireless Configuration
SSID DUT_B
Channel 0 - (2407 MHz)
Association Status Not Associated
RSSI (dBm) -
Mode Remote Router
Port Information
ETH A MAC Address 00:30:1A:1C:3D:9F
Radio A MAC Address 00:30:1A:1F:4C:62
ETH B MAC Address 00:30:1A:1C:3D:A0
Radio B MAC Address 00:30:1A:1F:49:73
Apply Changes

Figure 2-41 Remote Router/NAT Wireless IP Configuration

In order for the Remote Router/NAT device to associate with the Root Bridge device, the user needs to configure the Root Bridge's SSID and channel information for the Remote Router/NAT device.

Follow these steps below to configure the Remote Router/NAT Mode wireless association parameters:

1. From the 'Radio' dropdown menu, choose the radio that has to be configured with the wireless settings.
2. Enter the SSID and domain of the airHaul^2 Nexus PRO Root Bridge device.
3. Select the Transmit Power of the radio from Dial-a-Power dropdown menu
4. Select the gain of the antenna from the dropdown menu according to the gain of the antenna being used with the equipment
5. Enter the RF cable loss based on the cable specifications
6. Click '**Apply Changes**'. The units will attempt to associate.

Note: Clicking on **'Status'** will display further details on the association.

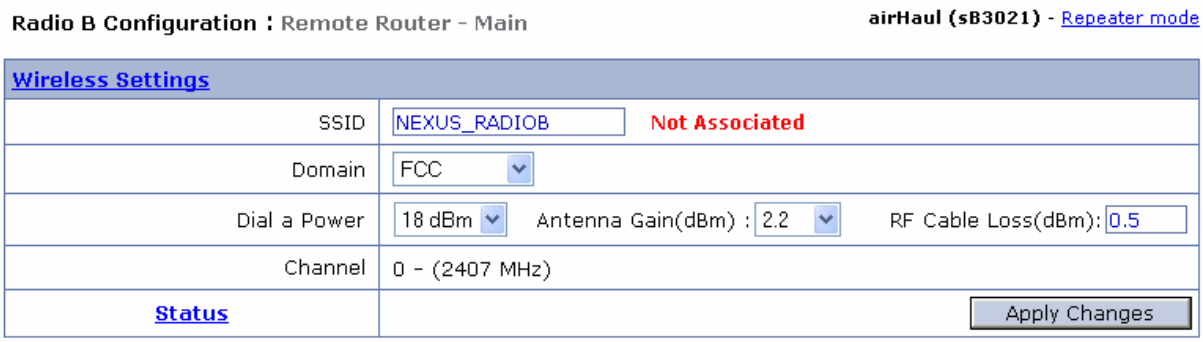


Figure 2-42 Remote Router/NAT Wireless Association Settings

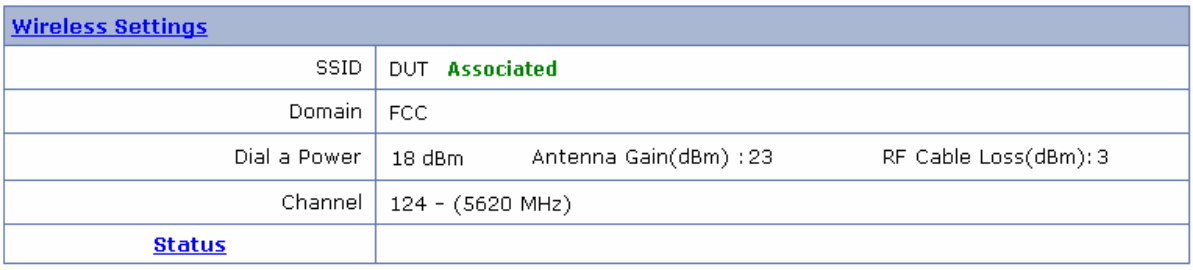


Figure 2-43 Remote Router/NAT Associated

Click on '**Status'** to view the association link-status graph.

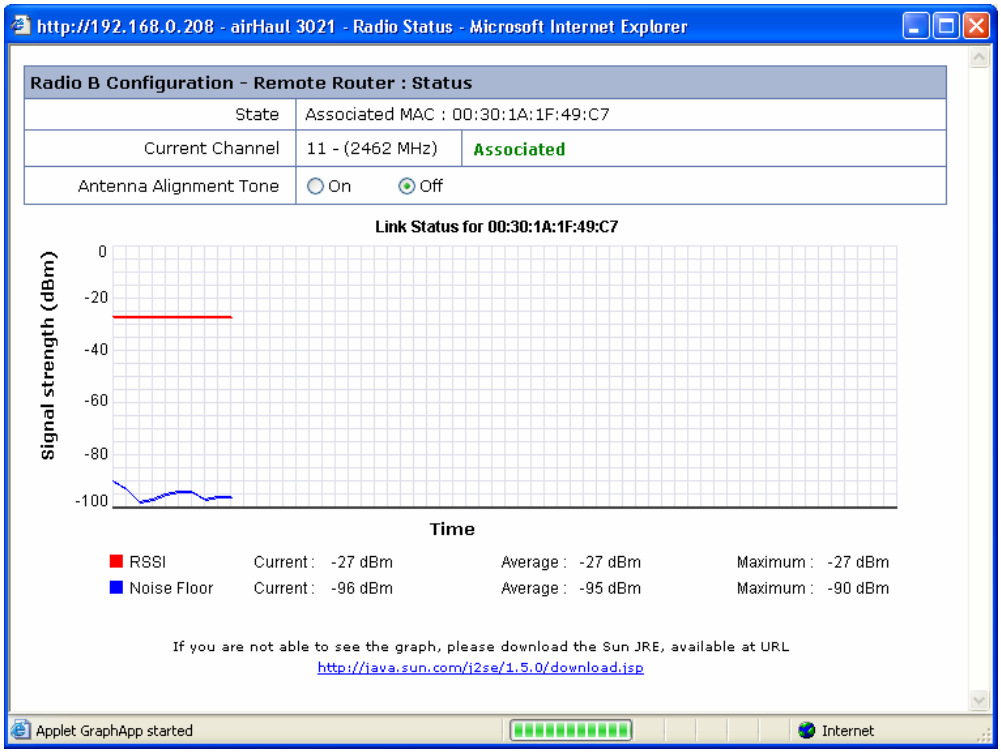


Figure 2-44 Link Status

Noise Floor is the measure of the signal created from the sum of all noise sources and unwanted signals within a measurement system.

Note: If the association status window does not appear, click on the link to download the JRE.

2.9.3 DHCP Configurations

The airHaul^2 Nexus PRO Remote Router/NAT unit can be used as a DHCP server or DHCP relay agent. DHCP (Dynamic Host Configuration Protocol) allows a host to be automatically assigned a new IP address out of a pool of IP addresses for its network.

A DHCP server/relay can only be configured when the device is in Remote Router/NAT Mode.

Follow the steps below to configure the Remote Router/NAT unit as a DHCP server:

1. Click on 'Networking' | '**DHCP Server**' from the menu bar to access the DHCP configuration page.
2. Click on 'Enable DHCP' to start the DHCP server configuration.
3. Enter the starting IP address for the IP pool range that can be assigned to a DHCP client.
4. Enter the maximum number of users for the maximum number of clients which can be assigned an IP address at a time by the DHCP server.
5. Enter maximum Lease Time in days, hours and minutes for all the clients.
6. Enter DNS Server IP address.
7. Click on the '**Apply Changes**' to change the settings

Note: The system will validate the input parameters and notify users of invalid entries.
The Starting IP address will be in the same network segment as the device wired-side Ethernet IP address.
IP address 0.0.0.0 for the DNS Server IP indicates no DNS Server to be used.
The DHCP Server is only available to hosts connected to the same LAN segment as the device wired-side Ethernet port.

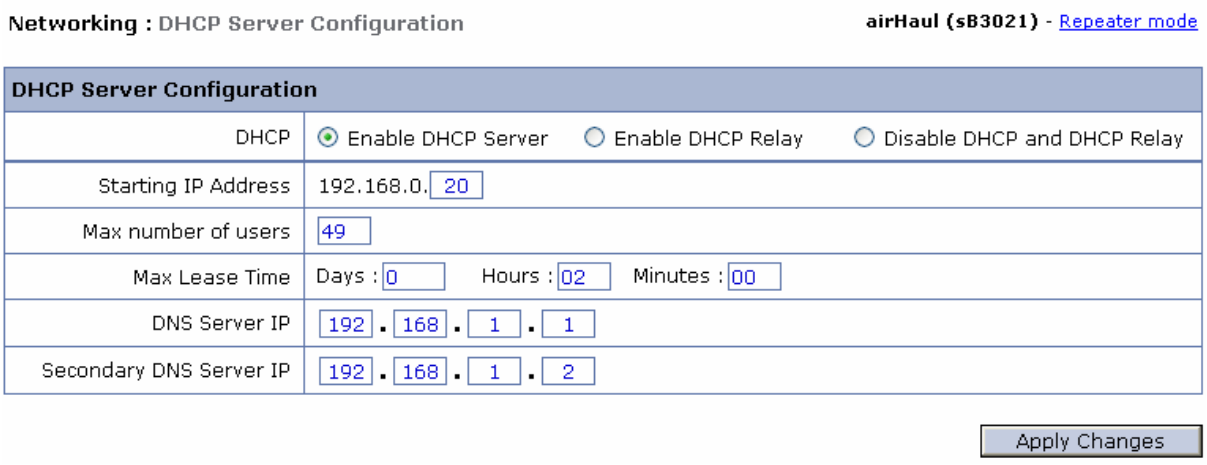


Figure 2-45 DHCP Server Configurations

Follow the steps below to disable the Remote Router/NAT DHCP server:

1. Click on **'Networking' | 'DHCP Server'** from the menu bar to access the DHCP configuration page.
2. Click on **'Disable DHCP and DHCP Relay'** to disable the DHCP server configuration.
3. Click on the **'Apply Changes'** button to change the settings

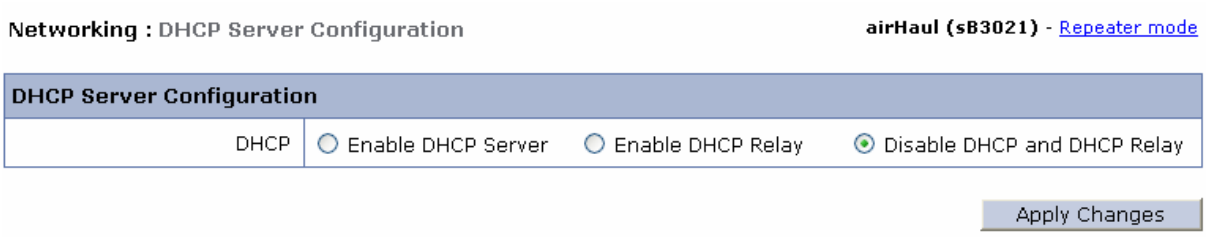


Figure 2-46 Disable DHCP and DHCP Relay

2.9.4 DHCP Relay Configurations

If the user has a DHCP Server, the airHaul^2 Nexus PRO Remote Router/NAT unit can be configured as a DHCP Relay agent of the DHCP Server for IP address assignment.

Follow the steps below to configure the Remote Router/NAT unit as a DHCP Relay Agent:

1. Click on **'Networking' | 'DHCP Server'** from the drop down menu to access the DHCP Configuration page.
2. Click on **'Enable DHCP Relay'** to choose DHCP Relay mode.
3. Enter a valid DHCP Server IP.
4. Click on the **'Apply Changes'** button to start the DHCP relay agent.

Note: The system will validate the input parameters and notify users of invalid entries.
The DHCP Server IP will be in the same network segment as the device wireless Radio IP address.
The DHCP Server needs to be configured to serve IP range of the wired side Ethernet IP.
The DHCP Relay Agent is only available to hosts connected to the same LAN segment as the device wired-side Ethernet port.

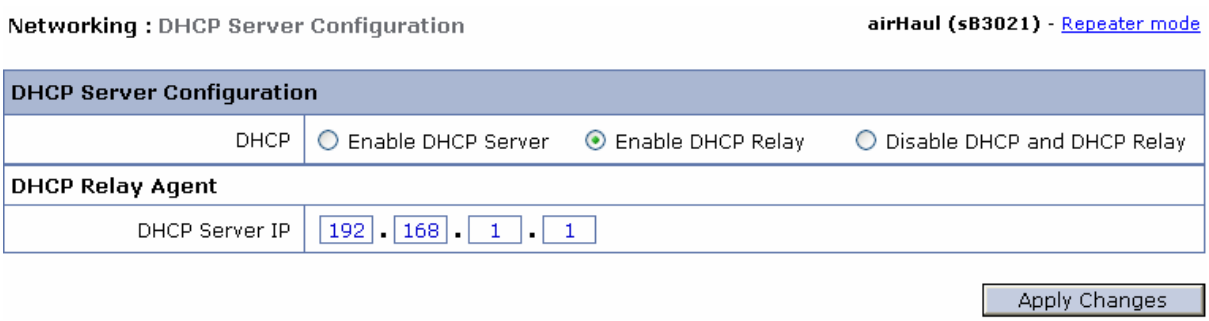


Figure 2-47 DHCP Relay Agent Configurations

Follow the steps below to disable the Remote Router/NAT DHCP Relay Agent:

1. Click on **'Networking' | 'DHCP Server'** from the menu bar to access the DHCP configuration page.
2. Click on **'Disable DHCP and DHCP Relay'** to disable the DHCP server configuration.
3. Click on **'Apply Changes'** to change the settings.

2.9.5 Routing Table

The web interface allows viewing of the routes and the addition and removal of the static routes for the Remote Router/NAT. The Routing Table is common to all the operating modes.

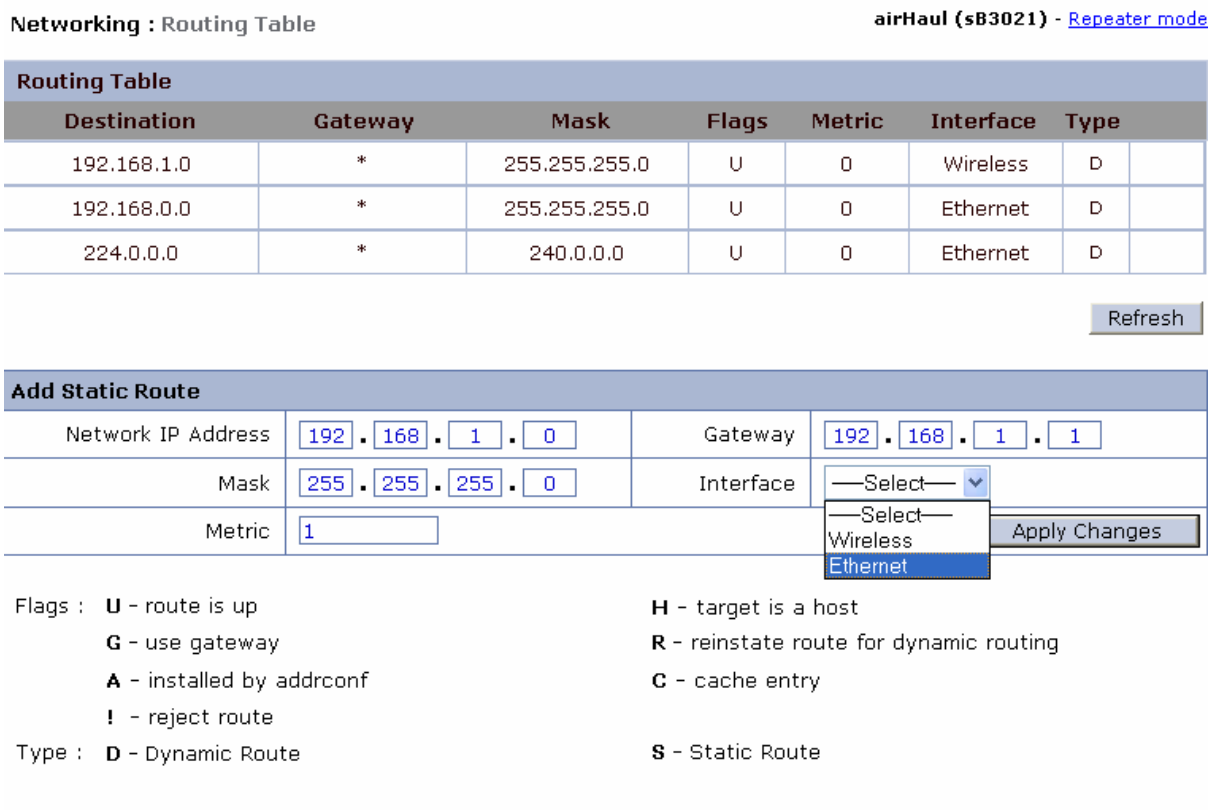


Figure 2-48 Adding a Route in the Routing Table

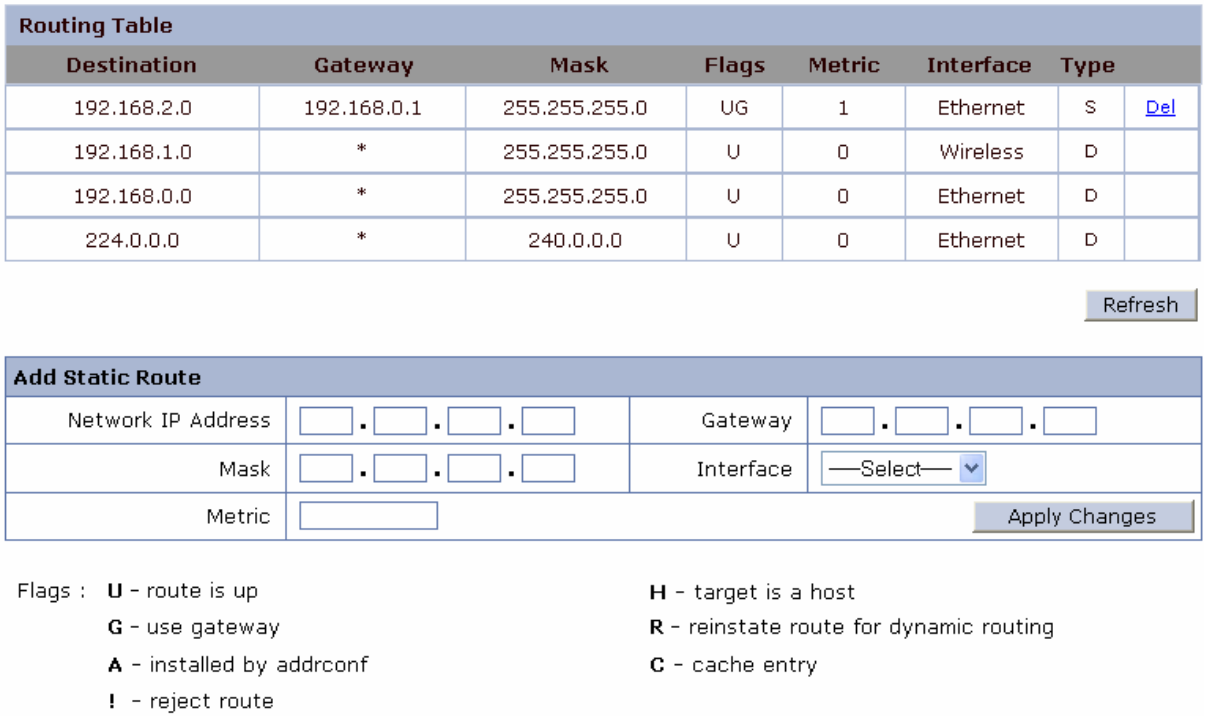

Routing Table
Destination Gateway Mask Flags Metric Interface Type
192.168.2.0 192.168.0.1 255.255.255.0 UG 1 Ethernet S Del
192.168.1.0 * 255.255.255.0 U 0 Wireless D
192.168.0.0 * 255.255.255.0 U 0 Ethernet D
224.0.0.0 * 240.0.0.0 U 0 Ethernet D
Refresh
Add Static Route
Network IP Address
Gateway
Mask
Interface
—Select—
Metric
Apply Changes
Flags : U - route is up
H - target is a host
G - use gateway
R - reinstate route for dynamic routing
A - installed by addrconf
C - cache entry
! - reject route

Figure 2-49 Deleting a Route entry in the Routing Table

Follow these steps below to delete a static route entry in the Remote Router/NAT device.

1. Click on **'Networking' | 'Routing Table'** from the menu bar to access the view routing table page.
2. Click on **'Del'** on the right hand side of the route entry to be deleted.
3. Click on **'Apply Changes'** to delete the route.

Note: Only static routes can be deleted.

Follow these steps below to add a static route entry in the Remote Router/NAT device.

1. Click on **'Networking' | 'Routing Table'** from the menu bar to access the view routing table page.
2. Enter the Network IP, Mask, Gateway, Interface and Metric entry for the new route as shown in the Figure.
3. Click on **'Apply Changes'** to add the new static route.

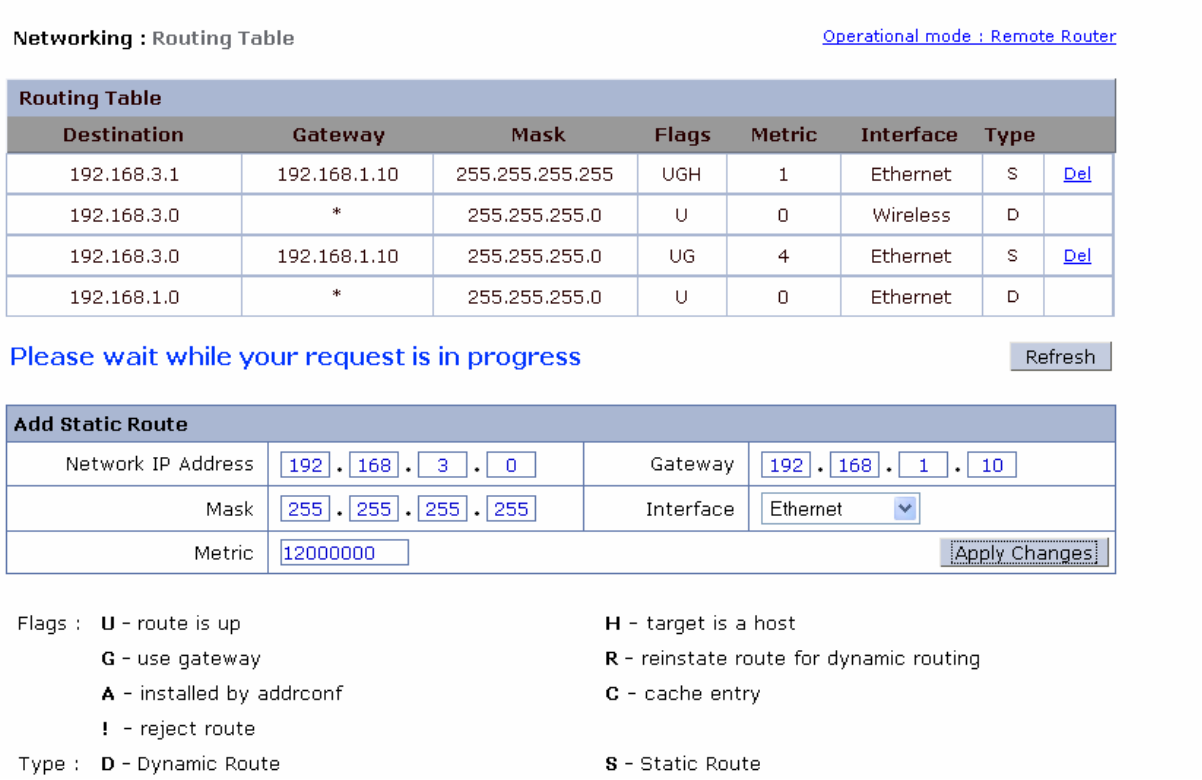

Networking : Routing Table
Operational mode : Remote Router
Routing Table
Destination Gateway Mask Flags Metric Interface Type
192.168.3.1 192.168.1.10 255.255.255.255 UGH 1 Ethernet S Del
192.168.3.0 * 255.255.255.0 U 0 Wireless D
192.168.3.0 192.168.1.10 255.255.255.0 UG 4 Ethernet S Del
192.168.1.0 * 255.255.255.0 U 0 Ethernet D
Please wait while your request is in progress
Refresh
Add Static Route
Network IP Address 192 . 168 . 3 . 0
Gateway 192 . 168 . 1 . 10
Mask 255 . 255 . 255 . 255
Interface Ethernet
Metric 12000000
Apply Changes
Flags : U - route is up
H - target is a host
G - use gateway
R - reinstate route for dynamic routing
A - installed by addrconf
C - cache entry
! - reject route
Type : D - Dynamic Route
S - Static Route

Figure 2-50 Adding Static Route

2.10 Disabling Radio for Single Radio Operation

The Dual Nexus PRO backhaul contains two Nexus PRO radios within a single enclosure for operational flexibility. However, single radio operation is also possible by disabling one radio and using the other as a Root Bridge, Remote Bridge, Remote Router/NAT or Remote NAT. The Disable Radio function is available only when the Device Operational Mode is set as Repeater Mode.

Note: If only one radio is needed, ensure that the other radio is disabled.

Follow the steps below to disable one of the radios:

1. Go to the System Configuration Page.
2. Click on the "**Current Operational Mode**" and select **Disable** from the dropdown menu of the radio to be disabled.
3. Click on the **Apply Changes button** to save the necessary configuration. Depending on the other radio configuration (Bridge or Router) a confirmation pop up IP settings window will appear.
4. Dial the necessary configuration and click on the **Apply Changes button** to save the configuration.

System Configuration	
System Name	Nexus
System Description	Nexus
SNMP Security	SNMP Security
Reset	Reset
Delayed Reset	Delayed Reset
NTP Server	NTP Server Settings Time Server Not available
Firmware Version	v0.00.05 Release Notes
Radio Firmware Version	1.1.2.17
Edit Configuration	IP Configuration Radio A : Performance Security Radio B : Performance Security
Reset To Factory Defaults	Reset To Defaults
Ethernet MTU Size	1512 bytes
Syslog server IP Address	0.0.0.0 Log level : -
SNMP Trap server IP Address	0.0.0.0
Watch Guard	Suspended for 2063 seconds Enable Suspend
Radar Scan	Disabled
LED Control	On

Current Operational Mode

Device Mode : Repeater mode

Radio A : Root Bridge mode **Radio B :** Disable Apply Changes

Root Bridge mode
Remote Bridge mode
Remote Router mode
Remote NAT mode

Figure 2-51 Disabling of one radio

Summary Information : **airHaul (sB3021)** - Root Bridge mode

Bridge IP Configuration (ETH A,ETH B,RADIO A)	
IP Address	192.168.0.208
IP Mask	255.255.255.0
Gateway	192.168.0.218
DHCP	Disabled

Port Information	
ETH A MAC Address	00:30:1A:1C:3D:9F
ETH B MAC Address	00:30:1A:1C:3D:A0
Radio A MAC Address	00:30:1A:1F:4C:62
Radio B MAC Address	00:30:1A:1F:49:73

Radio A: Wireless Configuration	
SSID	DUT A
Channel	11 - (2462 MHz)
RSSI (dBm)	-31
Maximum Wireless Throughput (Kbps)	30720
Mode	Root Bridge

Radio B: Wireless Configuration (Disabled)	
SSID	NEXUS_RADIOB
Channel	140 - (5700 MHz)
RSSI (dBm)	No Association
Maximum Wireless Throughput (Kbps)	30720
Mode	Disabled

Figure 2-52 Radio B Disabled

2.11. Wireless Settings Management

The Radio Configuration Main page can be accessed from the Radio menu. Its contents will be slightly different for each of the operating different modes.

2.11.1 Wireless Settings

Please refer to the Wireless Configuration sections for the different modes (Sections 2.7.2, 2.8.2 and 2.9.2).

2.11.2 Data Encryption

The different types of Data Encryption that can be configured on Root Bridge and Remote Router/NAT are as follows:

1. WEP Only
2. WPA –PSK
3. WPA2-PSK

Note: For Client Bridge, the default security is none. For Root Bridge, the default security is ACL+WEP.

WEP

Wireless Equivalent Privacy (WEP) encryption is used for security for the airHaul^2 Nexus PRO radio. To enable or disable WEP or change the relevant settings, the user can go to the security setting page on the web interface. The following table describes the information for the Data Encryption.

Table 2-5 Data Encryption

Page Items	Descriptions
Authentication	Selects authentication method between open system and shared key Open system: Open System is null authentication. With WEP enabled and valid WEP key on both ends, it provides data encryption. Clients without correct WEP key still can associate but can not send packet through. Shared key: Strict authentication for both authentication and data encryption. Clients must provide valid WEP key to associate.
WEP	Enable /Disable WEP Encryption
WEP Key Type	HEX
WEP Key Size	Chooses encryption key size between 40bits and 104bits When key size is changed, all 4 keys are lost and the user needs to re-enter. 64 bits: The user has to input 10 HEX digits. 128 bits: The user has to input 26 HEX digits.

Valid Key	Chooses which key in the key table is used for authentication: 1 – 4 This value must be match between the root device and the Client.
Key Table	Display / Set WEP keys A maximum of four keys can be set.

Follow the steps below to configure the Data Encryption parameters:

1. Click the **'Security'** link from the 'Radio Main' page of the desired radio.
2. Click the **'Enable'** button on the WEP.
3. Choose the Authentication as 'Open System' or 'Shared Key' by clicking on the radio button.
4. Choose a WEP Key Size (64 Bits or 128 Bits) from the dropdown menu. WEP key length is 10 characters for 64 Bits and 26 characters for 128 Bits.
5. Choose a Valid Key from the dropdown menu.
6. Enter the WEP key in the Key Table entries.
7. Click the **'Apply Changes'** button to change the settings.

Note: The system will validate the key entries and provide error or warning notifications. The user must enter the key indicated by the Valid Key selection.

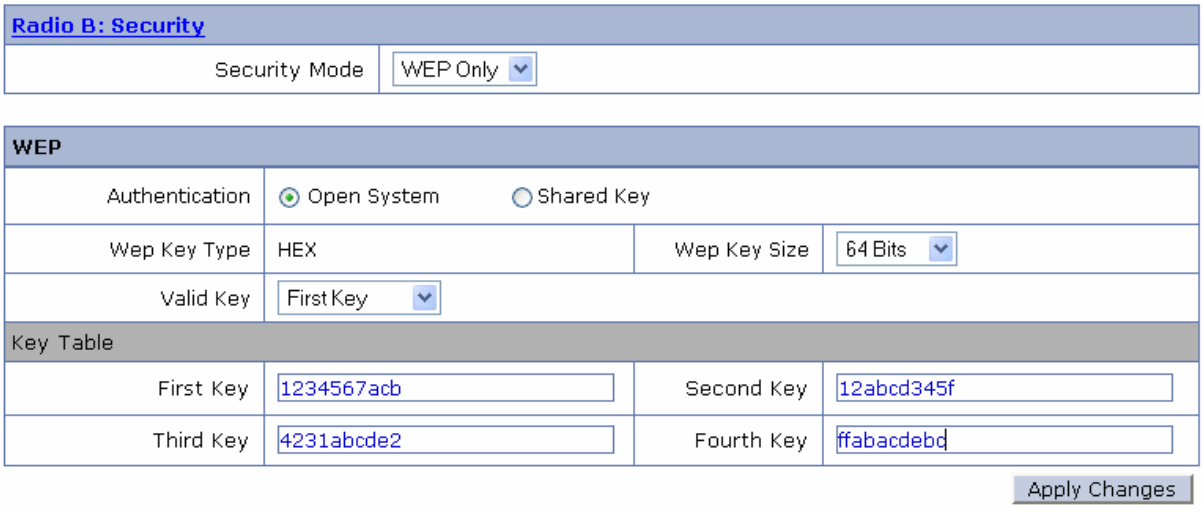


Figure 2-53 WEP Only Configuration

Follow the steps below to disable Data Encryption:

1. Click the **'Data Encryption'** link from the 'Radio Main' page.
2. If it is in **Shared key** mode, set to **Open System**.
3. Click the '**Disable** button on the WEP.
4. Click the **'Apply Changes'** button to change the settings.

WPA-PSK

To configure WPA-PSK, follow the steps below:

1. Click on the **RADIO A: Security** (similarly for Radio B Security).
2. Select the **WPA-PSK** from the dropdown menu of the Security Mode.
3. Dial the MAC that can be authenticated.
4. Enter the WPA Shared Key (between 8 to 64 characters) in the dialog box provided.
5. Enter the re-key time, by which the authentication is will be checked repeatedly.
6. Select the encryption type between TKIP and AES.
7. Click on **Apply changes** to save the configuration details.

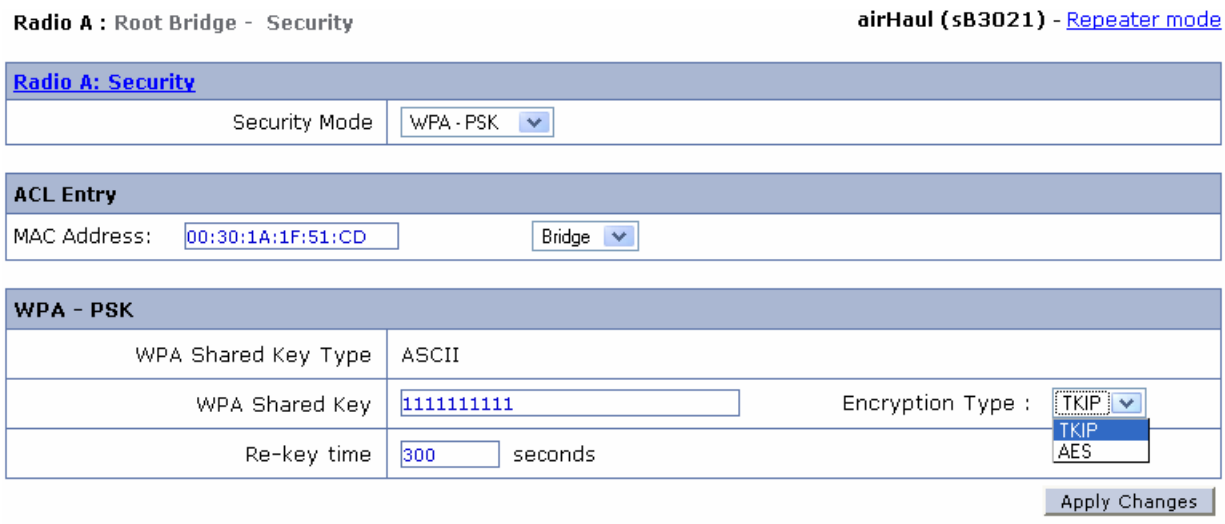


Figure 2-54 Configuring WPA-PSK

Table 2-6 WPA-PSK

Page Items	Descriptions
WPA-PSK	WPA-PSK is an extra-strong encryption where the encryption keys are automatically changed (called **re-keying**) and authenticated between devices after a specified period of time, or after a specified number of packets has been transmitted. WPA-PSK is far superior to WEP and provides stronger protection for the home/SOHO user for two reasons. The process used to generate the encryption key is very rigorous and the re-keying (or key changing) is done very quickly. This stops even the most determined hacker from gathering enough data to break the encryption.
WPA-Shared Key	The key that is used by the clients to get authenticated with the Root Bridge.
Re-key Time	The time period during which the keys will be re-negotiated.
MAC Address	MAC address of the client that can get authenticated

WPA2-PSK

Based on the 802.11i standard, WPA2 was released in 2004 and uses a stronger method of encryption. Like WPA, WPA2 offers two versions – Personal and Enterprise. Personal mode requires only an access point and uses a pre-shared key for authentication while Enterprise mode requires a RADIUS authentication server and uses EAP.

Note: Currently WPA2-PSK is using the TKIP as the encryption type.

Follow the steps below to configure the WPA2-PSK:

1. Click on **RADIO A: Security** (or **RADIO B: Security)**.
2. Select the **WPA2-PSK** from the dropdown menu of the Security Mode.
3. Dial the MAC that can get authenticated.
4. Enter the WPA Shared Key (between 8 to 64 characters) in the dialog box provided.
5. Select the encryption type between TKIP and AES.
6. Enter the Re-key time, by which the authentication is going to be checked repeatedly.
7. Click on **Apply changes** to save the configuration details.

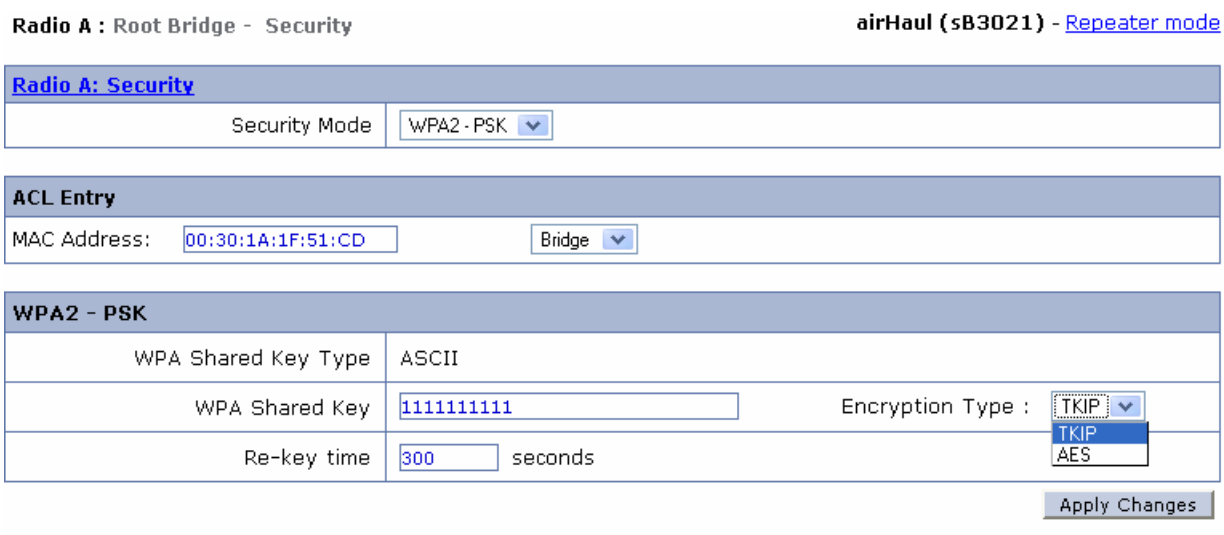


Figure 2-55 WPA2-PSK

3. Performance Parameters and Bandwidth Controller

This chapter gives instructions for editing the wireless radio protocol parameters to optimize radio performance and for changing the Bandwidth Controller. These procedures are the same for all the operational modes.

3.1 Link Performance Parameters and Features

The wireless radio performance parameters can be edited to optimize the radio performance. The radio protocol parameters are:

1. Fragment Length (between 256 and 2346)
2. RTS/CTS (between 256 and 2346)
3. RSSI Threshold (between -90 and -20)
4. Preamble Settings: Long, Short or Dynamic
5. Distance
6. Frame Bursting
7. Concatenation
8. Piggy Back
9. Radio Operating Mode
10. Throughput Optimizer

Performance			
Fragment Length (256 - 2346)	2346	RTS / CTS Length (256 - 2346)	2346
RSSI Threshold	-90	Preamble Settings	Long
Distance	150 Km		
Frame bursting	On	Concatenation	Off
Piggy back	Off		
Radio Operating mode	sB Enhanced Mode (Compression Off)		
Throughput Optimizer (0 - 10)	6		

Figure 3-1 Performance Settings

Table 3-1 Radio Performance Parameters

Page Item	Descriptions
Fragment Length	a) Shows current value b) Changes to a value within its range This setting determines the size at which packets are fragmented. If the frame that the access point is transmitting is larger than the threshold, it will trigger the fragmentation function. The use of fragmentation can increase the reliability of frame transmissions. Because smaller frames are being sent, collisions are much less likely to occur.

Page Item	Descriptions
	Default value is 2346 bytes. The range of value is from 256 to 2346.
RTS/CTS Length	a) Shows current value b) Changes value RTS: Request To Send CTS: Clear To Send The RTS/CTS length determines the packet size at or larger than the set value. The radio issues a request to send (RTS) before sending the packet. The primary reason for implementing RTS/CTS is to minimize collisions among hidden stations. Default value is 2346 bytes. The range of value is from 256 to 2346.
RSSI Threshold	This function provides better performance in high noise area. The device will ignore any signal below the set RSSI threshold. The default value is -90. The value ranges from -90 to -20.
Preamble Settings	a) Shows current value b) Chooses other settings available in the dropdown menu The radio preamble is a section of data at the head of a packet that contains information the Root Device and Remote devices need when sending and receiving packets. The dropdown menu allows the user to select a long, short or dynamic radio preamble. The default is dynamic. Long: a long preamble provides a stable link Short: a short preamble improves throughput performance. But it only allows short preamble capable Remotes to be associated. Dynamic: a dynamic preamble allows mixing of short and long preambles
Distance	The appropriate distance between the Root and the Remote devices needs to be configured for best results. The range of the link, which corresponds to the ACK window size.
Frame Bursting	Short 802.11g packets can be unwrapped and rebundled into a larger packet to reduce the impact of mandatory gaps between the packets. This increases the speed of the 802.11g based wireless networks. Frame bursting is sometimes also called “packet bursting”.
Concatenation	The benefit of concatenation is that it increases the throughput by removing overheads from “extra” frames and interframe latencies.
Piggy Back	Piggy Back is a performance boosting feature which increases the effective transmission speed with no intervention.

Page Item	Descriptions
	According to the IEEE 802.11 standard specification, a single frame combining a plurality of information can be transmitted. For example, the frame may carry data+acknowledgement (ACK), data+poll , data+ ACK +poll or ACK +poll for transmission. Using the piggy back increases the communication efficiency, depending on the transfer medium or size of data being transferred. **Note**: It can be used for improved performance with compatible devices. (May not be compatible with third party devices).
Radio Operating mode	sB Enhanced Mode gives better performance with the compression option. For this reason, it does not support 802.11b.
Throughput Optimizer	The Throughput Optimizer is used to optimize the radio link speed and performance. The valid range is 0 to 10. The default value is 6. Setting a higher value will cause the radio to attempt to establish at the highest possible data rate in an aggressive way. A smaller "Throughput Optimizer" value means a more stable link. **Note**: The default value for the Throughput Optimizer is 6. Vary the Throughput Optimizer settings to achieve a more stable link.

Follow the steps below to change the Radio Performance:

1. From the **Radio Configuration** page click on the **Performance** link.
2. Enter the **Fragment Length**.
3. Input the desired **RTS/CTS Length**.
4. Choose the **Preamble Settings** from the dropdown list.
5. Enter the **Distance** of the Remote Device.
6. Turn ON/OFF **Frame Bursting**.
7. Turn ON/OFF **Concatenation**.
8. Turn ON/OFF **Piggy Back**.
9. Choose the desired **Radio Operating Mode**
10. Select an appropriate value for the **Throughput Optimizer**.
11. Click on the **Apply Changes** button to effect the changes.

3.2 Bandwidth Controller

Using the bandwidth controller on the root device, the user can limit the wireless link bandwidth in the egress direction. To effectively control the upload and download bandwidth, the user will need to specify the necessary bandwidth parameters on both the airHaul^2 Nexus PRO devices.

The user can key in the maximum bandwidth of the wireless link allowed if the feeding bandwidth is adequate.

Follow the steps below to change the bandwidth parameters:

1. From the menu bar click on **Networking** | **Bandwidth Controller** dropdown menu item.
2. Click on the **Enable** radio button.
3. Enter **Maximum Wireless Throughput** for the egress traffic.
4. Click on the **Apply Changes** button to change the settings.

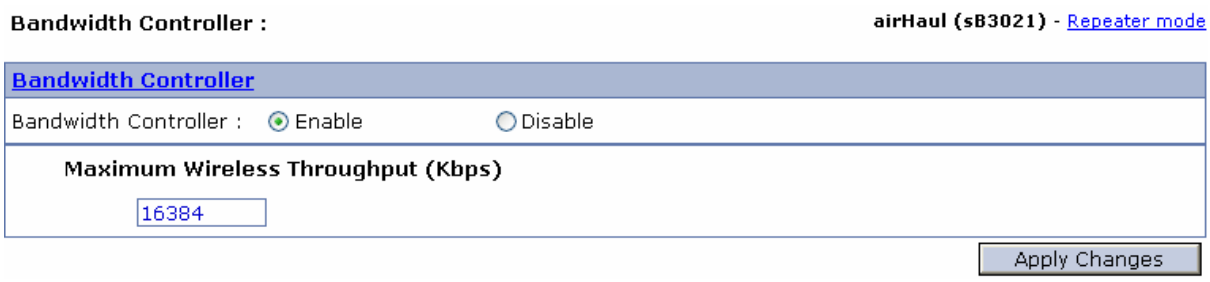


Figure 3-2 Bandwidth Controller

4. Quality of Service (QoS)

The primary goal of QoS is to provide priority such as dedicated bandwidth, controlled jitter and latency (required by some real time and interactive traffic), and improved loss characteristics. Another important goal is ensuring that by providing priority for one or more flows does not make compromise other flows.

QoS in 802.11 is defined by the IEEE 802.11e set of standards. Wireless Multimedia Extensions (WME), also known as Wi-Fi Multimedia (WMM) is a Wi-Fi Alliance certification based on this IEEE 802.11e. WMM prioritizes traffic according to 4 AC (Access Categories) - voice, video, best effort, and background. However, it does not provide guaranteed throughput. It is suitable for interactive applications that require QoS, such as Wi-Fi Voice over IP (VoIP).

Follow the steps below to Enable QoS:

1. From the menu bar click on **Networking** | **QoS** drop down menu item.
2. Click on **"QoS"** Enable radio button. A confirmation window pops up as shown in the figure below.

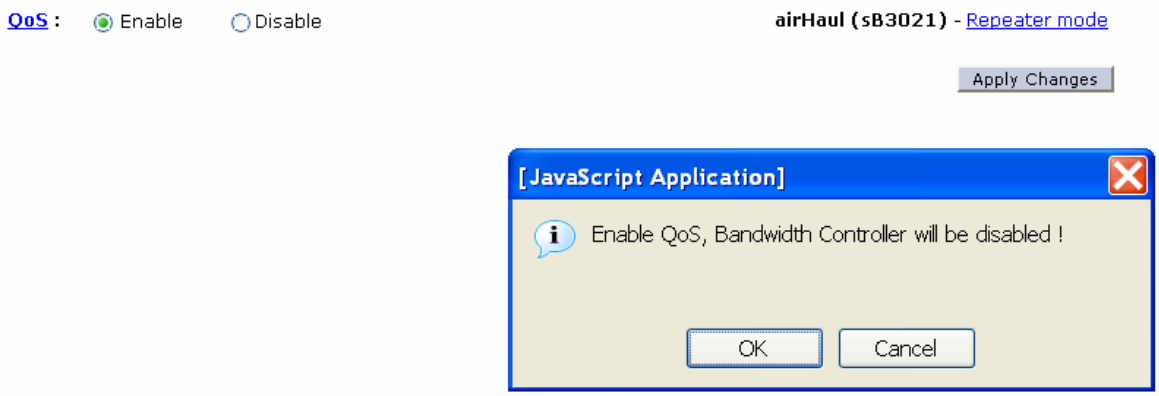


Figure 4-1 Enabling QoS

QoS : Enabled airHaul (sB3021) - Repeater mode

QoS Classes					
Class	Min Bandwidth (Kbps)	Max Bandwidth (Kbps)	Priority	Enable	
1)	10	30720			
2)	10	30720	0	Enabled	Filters
3)	10	30720	0	Enabled	Filters
4)	10	30720	0	Enabled	Filters
5)	10	30720	0	Enabled	Filters
6)	10	30720	0	Enabled	Filters
7)	10	30720	0	Enabled	Filters
8)	10	30720	0	Enabled	Filters
9)	10	30720	0	Enabled	Filters

Note : **class 1** indicates default value Priority '0' indicates "Best Effort"

Figure 4-2 QoS Front Page

Altogether, we have 9 different classes, which can be configured.

Note: Class 1 indicates the default value.

In order to define the filters for a class, follow the steps below:

1. Click on **Filters**.
2. Select the application packet that has to be filtered.

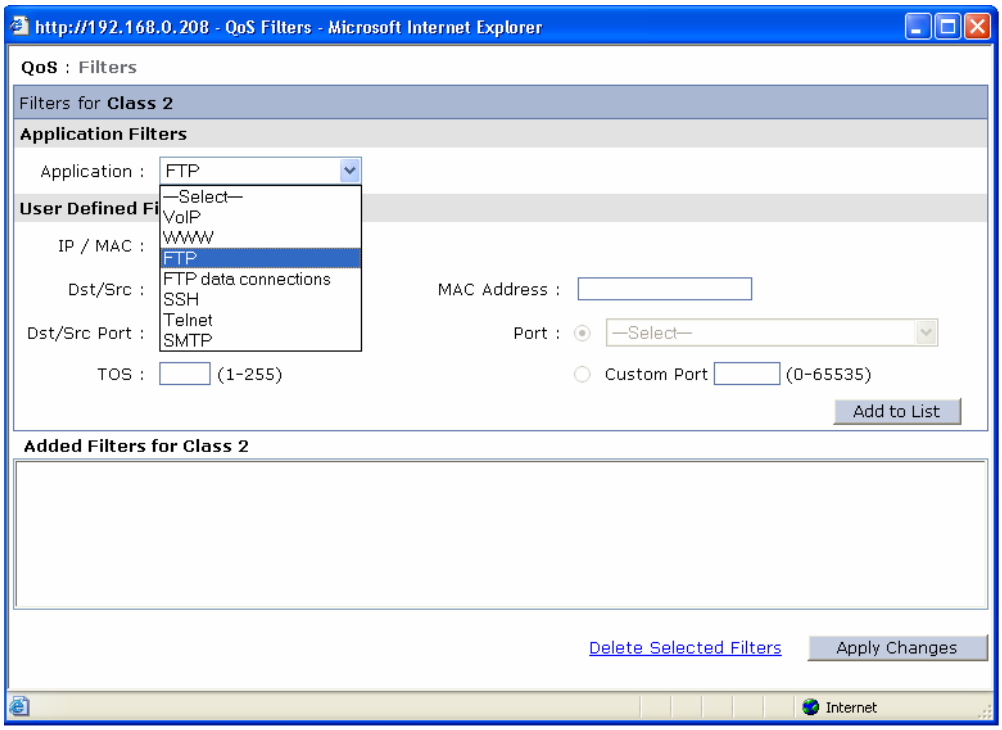


Figure 4-3 Selection Menu of Application Filter

3. Select whether the packet has to be filtered based on IP or MAC.

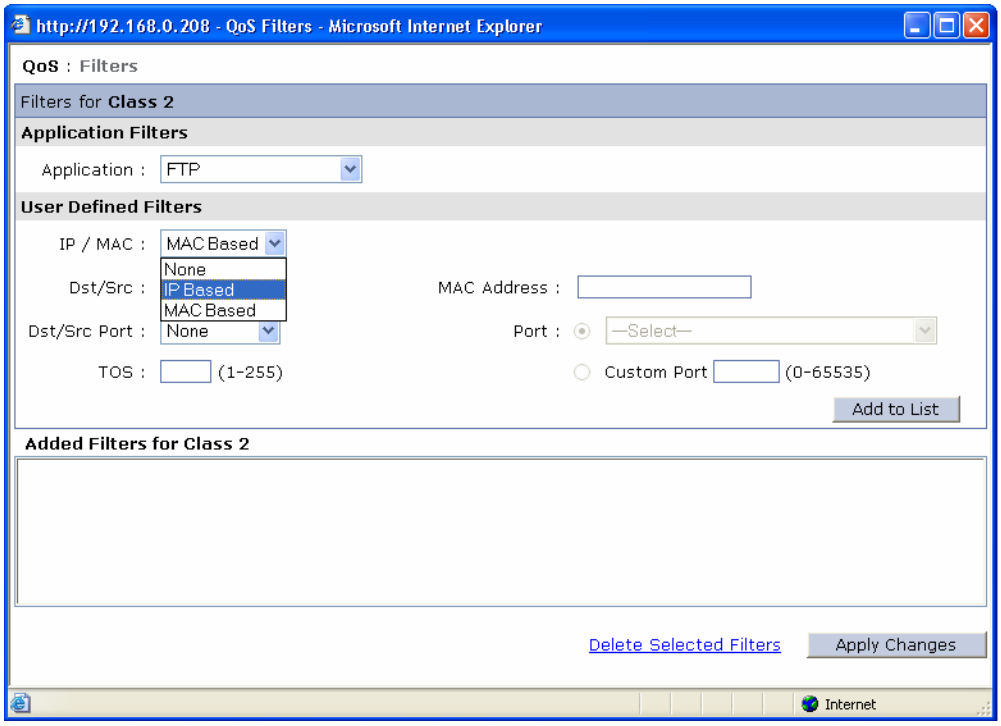


Figure 4-4 Selection Menu of IP/MAC based filter

4. Select whether the packet has to be filtered based on Source address or the Destination address.
   If the packet being filtered is based on IP, then enter the IP address. Or if it is filtered based on the MAC, then enter the MAC address.

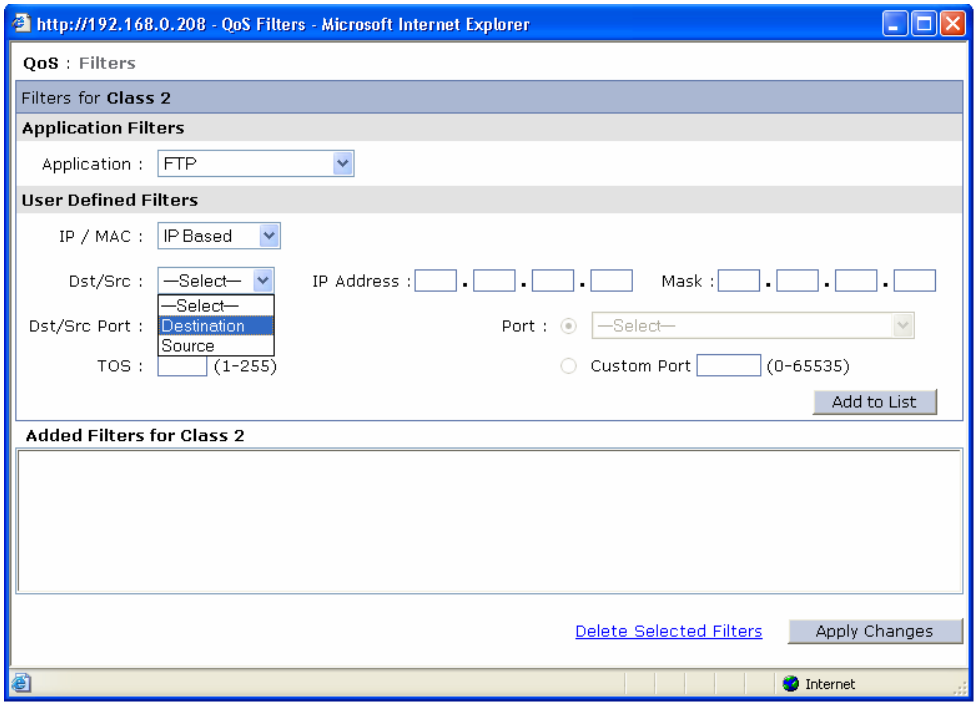


Figure 4-5 Selection Menu of Source/Destination Based Filter

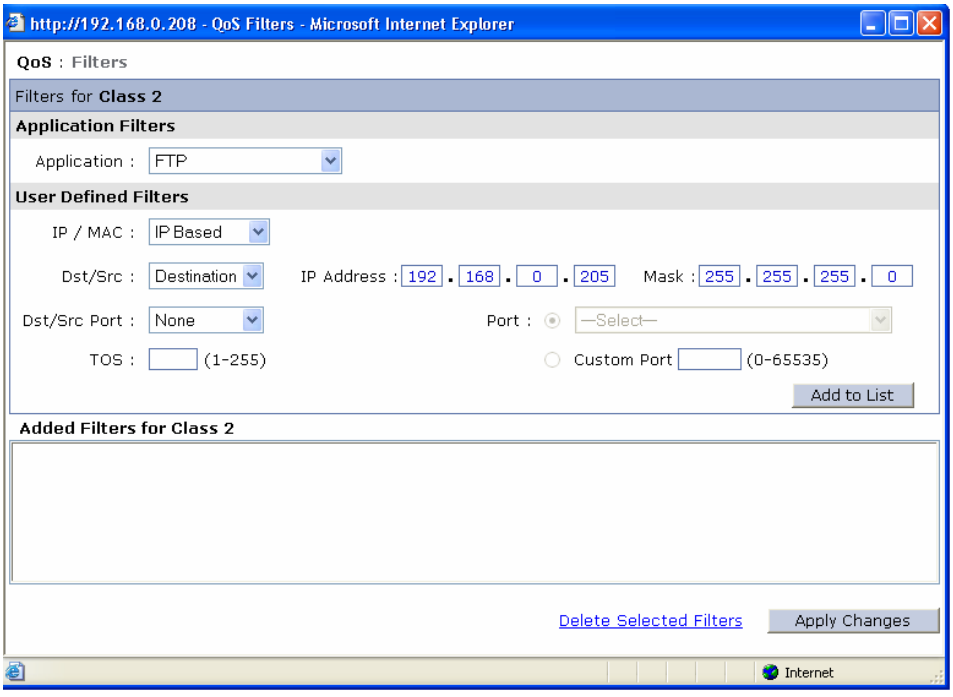

http://192.168.0.208 - QoS Filters - Microsoft Internet Explorer
QoS : Filters
Filters for Class 2
Application Filters
Application : FTP
User Defined Filters
IP / MAC : IP Based
Dst/Src : Destination
IP Address : 192 . 168 . 0 . 205
Mask : 255 . 255 . 255 . 0
Dst/Src Port : None
Port : —Select—
TOS : (1-255)
Custom Port (0-65535)
Add to List
Added Filters for Class 2
Delete Selected Filters
Apply Changes
Internet

Figure 4-6 IP Address Dialog Box

5. Select the Port, either Destination or Source based and select the Port Number from the drop down menu. Alternatively, the Port Number can be customized.

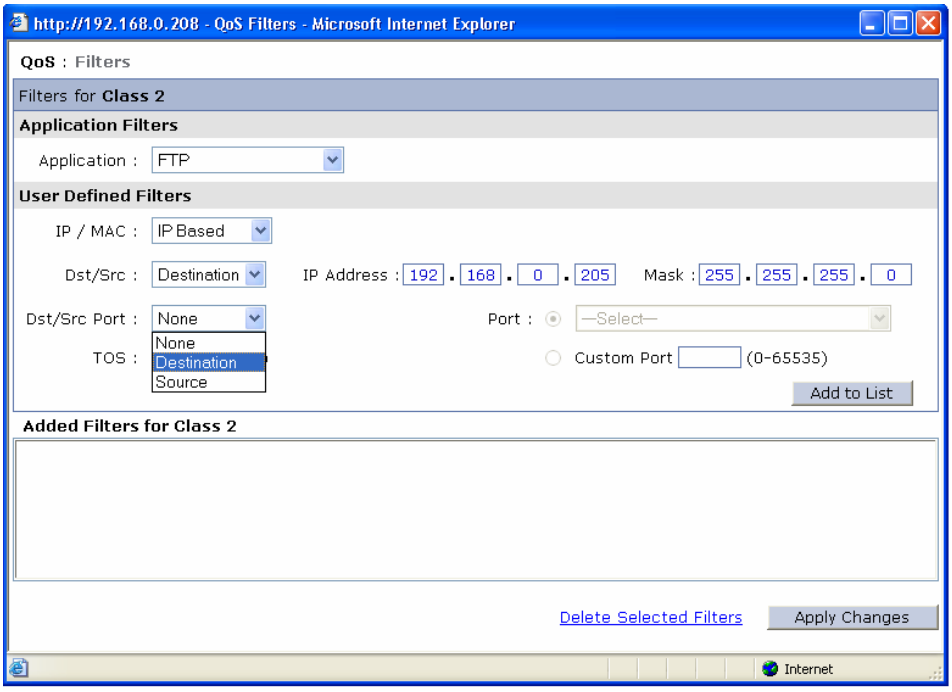


Figure 4-7 Selection of Destination/Source Port

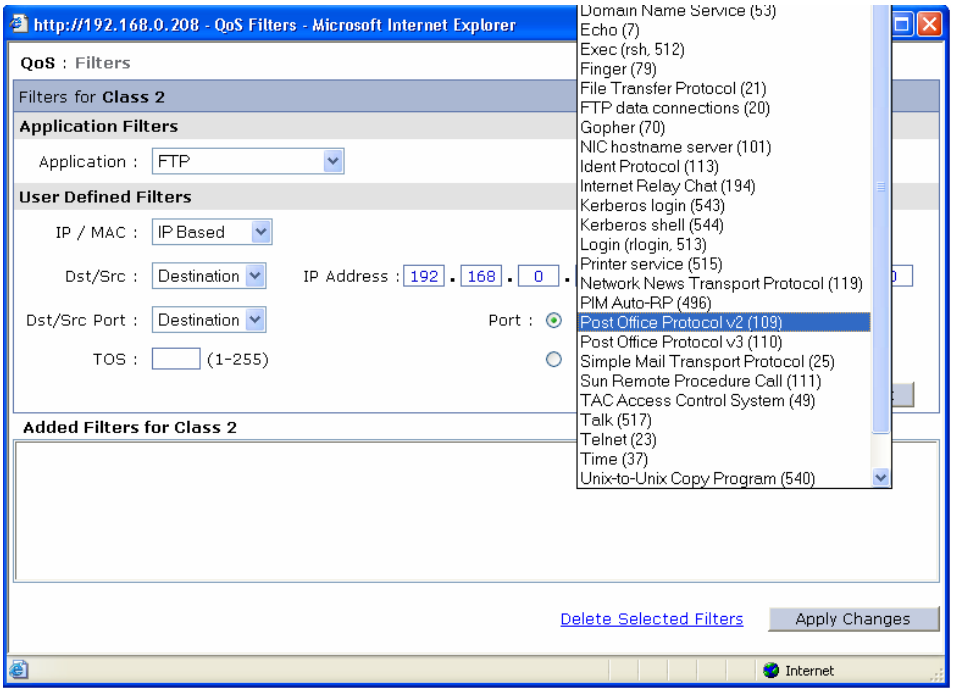


Figure 4-8 Selection Menu for Port Type (can be customized by user with the port number)

6. Assign the TOS value between 1 and 255.

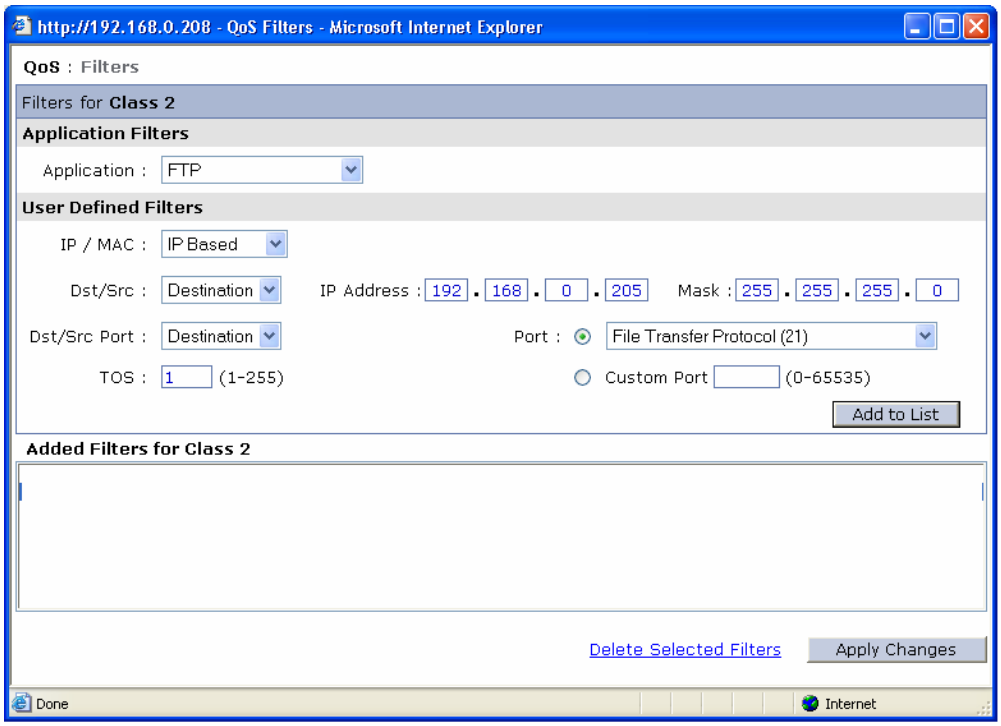

http://192.168.0.208 - QoS Filters - Microsoft Internet Explorer
QoS : Filters
Filters for Class 2
Application Filters
Application : FTP
User Defined Filters
IP / MAC : IP Based
Dst/Src : Destination
IP Address : 192 . 168 . 0 . 205
Mask : 255 . 255 . 255 . 0
Dst/Src Port : Destination
Port : File Transfer Protocol (21)
TOS : 1 (1-255)
Custom Port (0-65535)
Add to List
Added Filters for Class 2
Delete Selected Filters
Apply Changes
Done
Internet

Figure 4-9 TOS value Dialog Box

7. After configuring the user defined filter, click on the **Add to List** to add the selected filter.

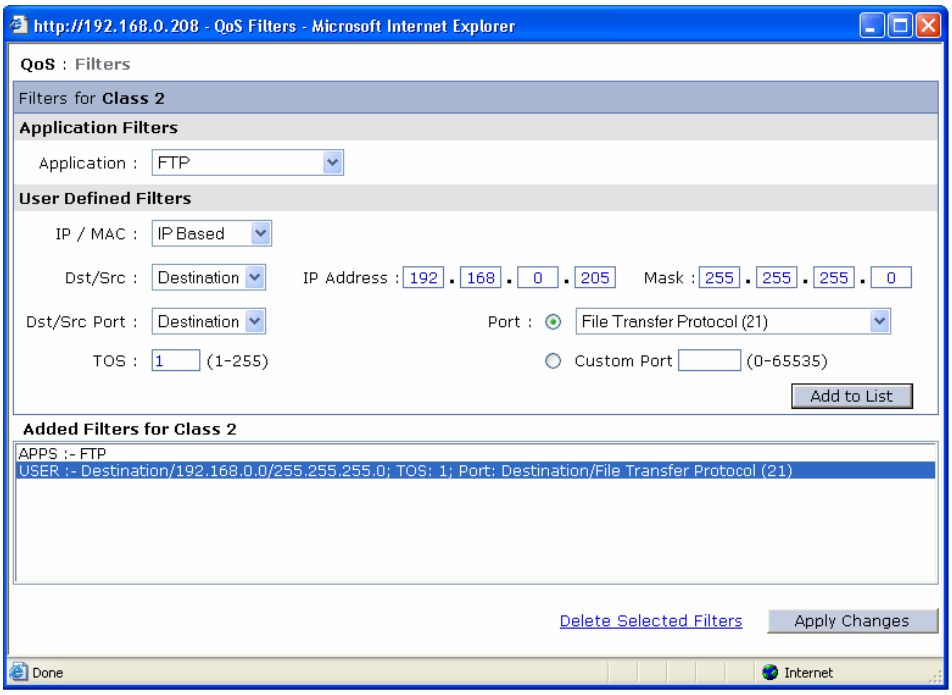

http://192.168.0.208 - QoS Filters - Microsoft Internet Explorer
QoS : Filters
Filters for Class 2
Application Filters
Application : FTP
User Defined Filters
IP / MAC : IP Based
Dst/Src : Destination
IP Address : 192 . 168 . 0 . 205
Mask : 255 . 255 . 255 . 0
Dst/Src Port : Destination
Port : File Transfer Protocol (21)
TOS : 1 (1-255)
Custom Port (0-65535)
Add to List
Added Filters for Class 2
APPS :- FTP
USER :- Destination/192.168.0.0/255.255.255.0; TOS: 1; Port: Destination/File Transfer Protocol (21)
Delete Selected Filters
Apply Changes
Done
Internet

Figure 4-10 Selected filter list window

8. After adding the desired filters to the list, Click on the **Apply Changes** to save the configuration of the filters. There will be a confirmation pop up window. Click **OK** to confirm or **Cancel** to discard the selection.

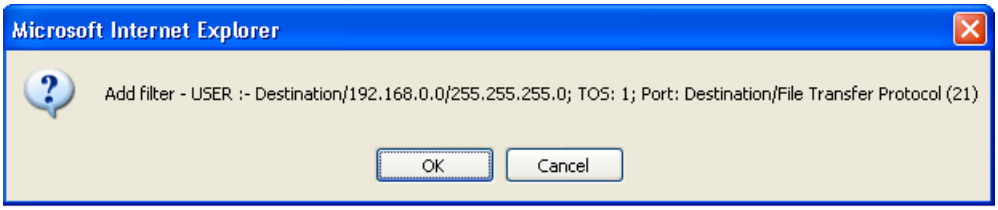

Microsoft Internet Explorer
Add filter - USER :- Destination/192.168.0.0/255.255.255.0; TOS: 1; Port: Destination/File Transfer Protocol (21)
OK
Cancel

Figure 4-11 Add filter Confirmation pop up window

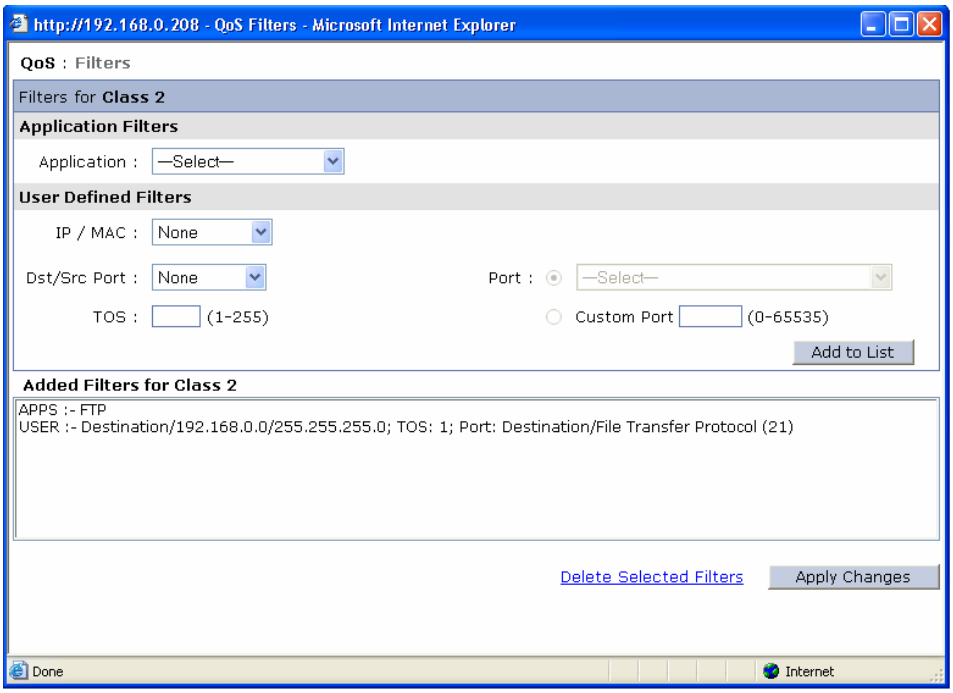


Figure 4-12 Added Filters

Deleting Filters:

1. The filters added can be deleted by first selecting the added filters from the list and then clicking on **Delete Selected filters**.

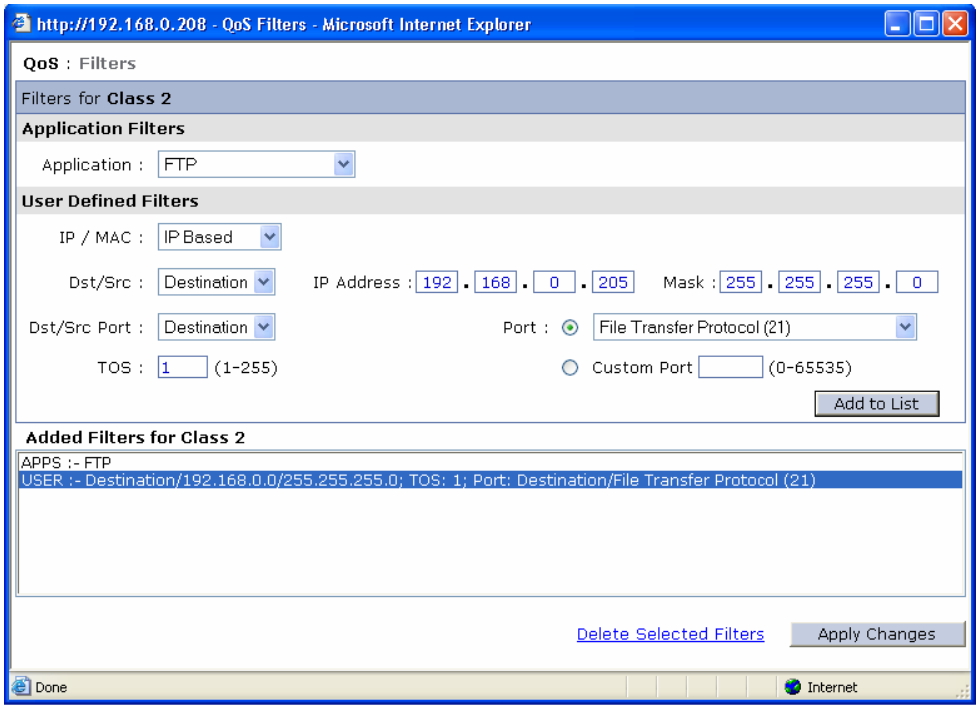

http://192.168.0.208 - QoS Filters - Microsoft Internet Explorer
QoS : Filters
Filters for Class 2
Application Filters
Application : FTP
User Defined Filters
IP / MAC : IP Based
Dst/Src : Destination
IP Address : 192 . 168 . 0 . 205
Mask : 255 . 255 . 255 . 0
Dst/Src Port : Destination
Port : File Transfer Protocol (21)
TOS : 1 (1-255)
Custom Port (0-65535)
Add to List
Added Filters for Class 2
APPS :- FTP
USER :- Destination/192.168.0.0/255.255.255.0; TOS: 1; Port: Destination/File Transfer Protocol (21)
Delete Selected Filters
Apply Changes
Done
Internet

Figure 4-13: Delete Selected Filters.

In order to configure the desired Minimum and Maximum bandwidth, priority across classes or disable certain classes:

1. Go to the QOS main page, click on the "**QoS**", the page appears as shown in the figure below.
2. Key in the desired bandwidth inside the dialog box of Minimum and Maximum Bandwidth
3. Use the scroll bar to select the desired priority for a particular class.
4. In order to enable a particular class, click on the radio button. A tick mark indicates that the particular class is enabled. In order to disable, click on the radio button and the tick mark disappears indicating that the class is disabled.
5. Finally after configuring, click on the "**Apply changes**" to save the configuration.

Note: 0 indicates default priority (Best effort).

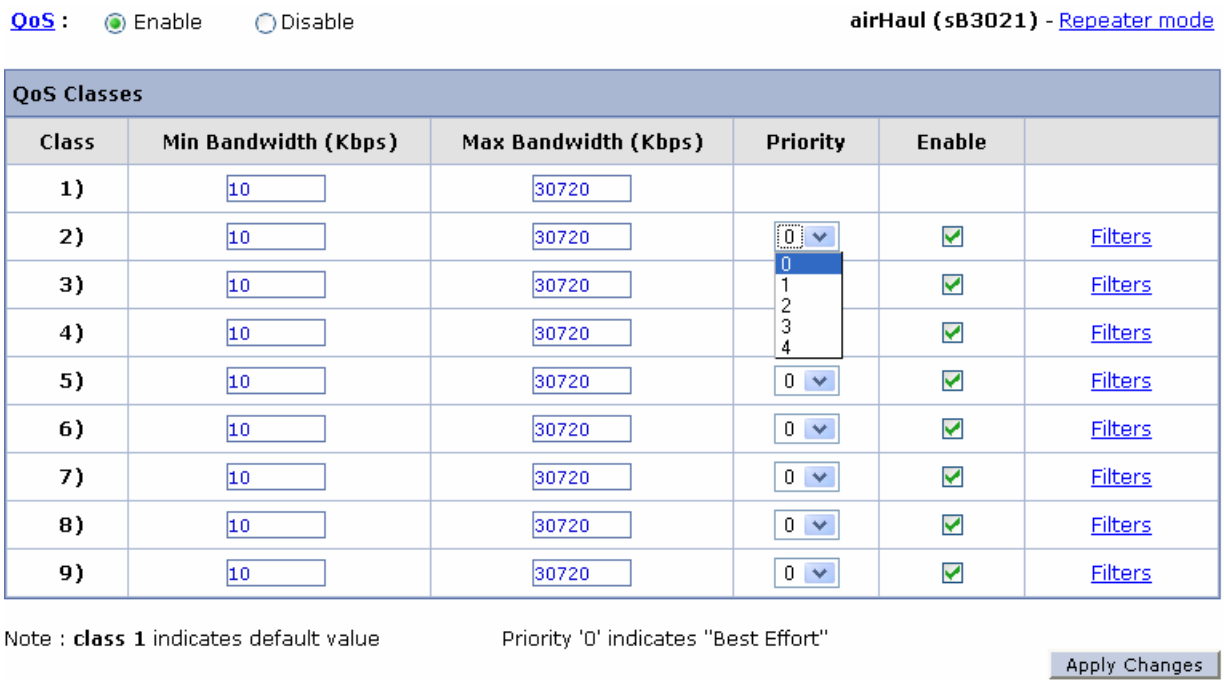


Figure 4-14 QoS Configuration Page

5. Survey

The **Site Survey** tool is available for airHaul^2 Nexus PRO units operating in Remote mode.

To access the site survey page, go to '**Tools**' | '**Site Survey**' drop down menu. The following figure shows the list of SSID from the site survey. It helps to select the root device with which the remote can associate. In order to associate with any of the devices in the list, click on the corresponding radio button and press the '**Associate**' button.

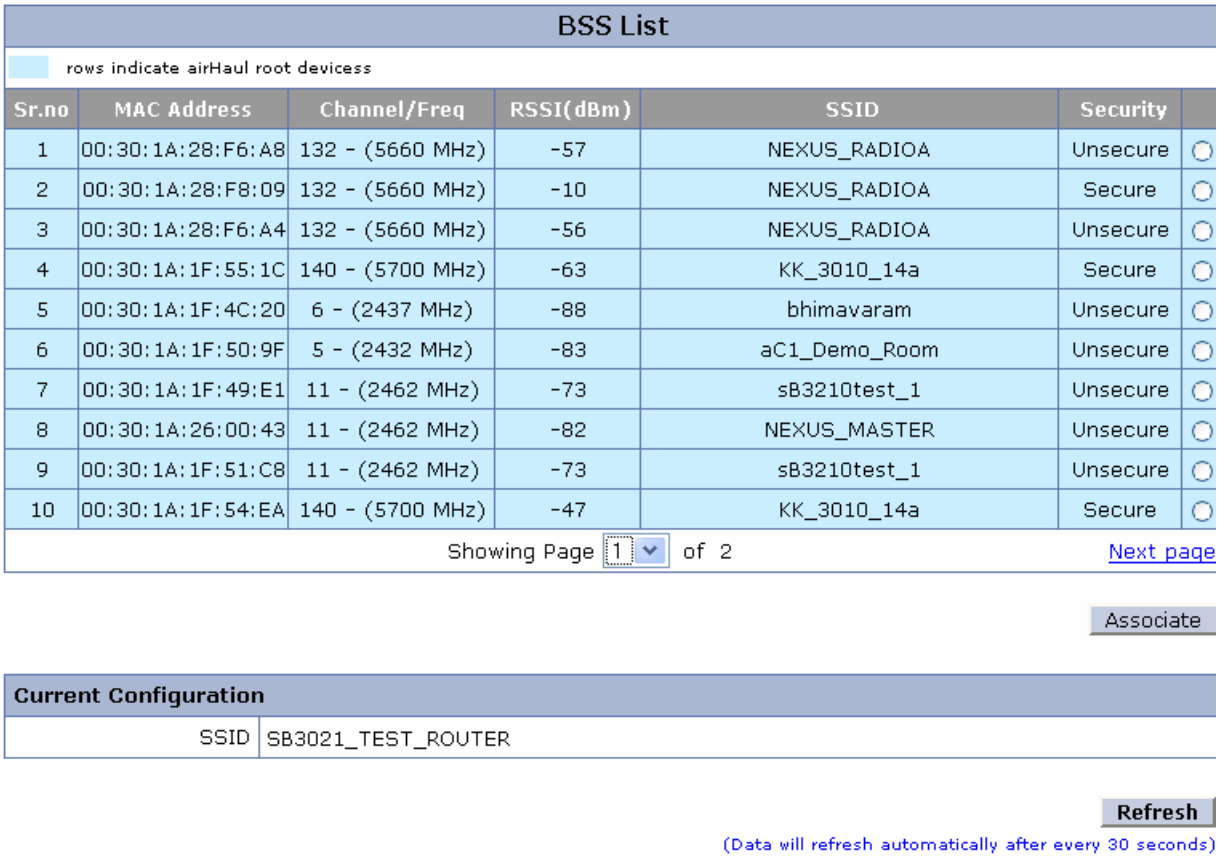

BSS List
rows indicate airHaul root devicess
Sr.no
MAC Address
Channel/Freq
RSSI(dBm)
SSID
Security
1 00:30:1A:28:F6:A8 132 - (5660 MHz) -57 NEXUS_RADIOA Unsecure
2 00:30:1A:28:F8:09 132 - (5660 MHz) -10 NEXUS_RADIOA Secure
3 00:30:1A:28:F6:A4 132 - (5660 MHz) -56 NEXUS_RADIOA Unsecure
4 00:30:1A:1F:55:1C 140 - (5700 MHz) -63 KK_3010_14a Secure
5 00:30:1A:1F:4C:20 6 - (2437 MHz) -88 bhimavaram Unsecure
6 00:30:1A:1F:50:9F 5 - (2432 MHz) -83 aC1_Demo_Room Unsecure
7 00:30:1A:1F:49:E1 11 - (2462 MHz) -73 sB3210test_1 Unsecure
8 00:30:1A:26:00:43 11 - (2462 MHz) -82 NEXUS_MASTER Unsecure
9 00:30:1A:1F:51:C8 11 - (2462 MHz) -73 sB3210test_1 Unsecure
10 00:30:1A:1F:54:EA 140 - (5700 MHz) -47 KK_3010_14a Secure
Showing Page 1 of 2
Next page
Associate
Current Configuration
SSID SB3021_TEST_ROUTER
Refresh
(Data will refresh automatically after every 30 seconds)

Figure 5-1 Site Survey showing associated devices

6. Antenna Alignment

Antenna Alignment can be used to optimize the radio performance and check the RSSI. This is only available when it is in Remote device mode. To access the antenna alignment, go to the menu bar under **Tools** and choose '**Antenna Alignment**'. Use the Wireless Settings to associate the Remote (Router or Bridge mode) with a Root device.

Click on the '**Status**' link to go to the Antenna Alignment page. The Link Status page will be displayed as shown below.

RSSI Audio Tones are provided to help the user align the antenna without looking at the link status display. Click on the '**Antenna Alignment Tone On**' button to hear the alignment tones. For more information on antenna alignment, please refer to the Quick Installation Guide.

To perform the antenna alignment:

1. Go to the menu bar and choose the '**Radio**' menu item.
2. From the Radio page, use the Wireless Settings to associate to the Root device
3. Click on the 'Status' link to go to the Antenna Alignment page. The Link Status page will be displayed as shown below. In the case of Root Bridge, click '**View Association Table'** to view the associated client.
4. A set of tones are provided to help the user align the antenna without looking at the link status display
5. Click on the '**Antenna Alignment Tone' "ON"** button to hear the alignment tones.

Note: Different pitch levels indicate a different RSSI value. The higher the pitch the higher the RSSI value.

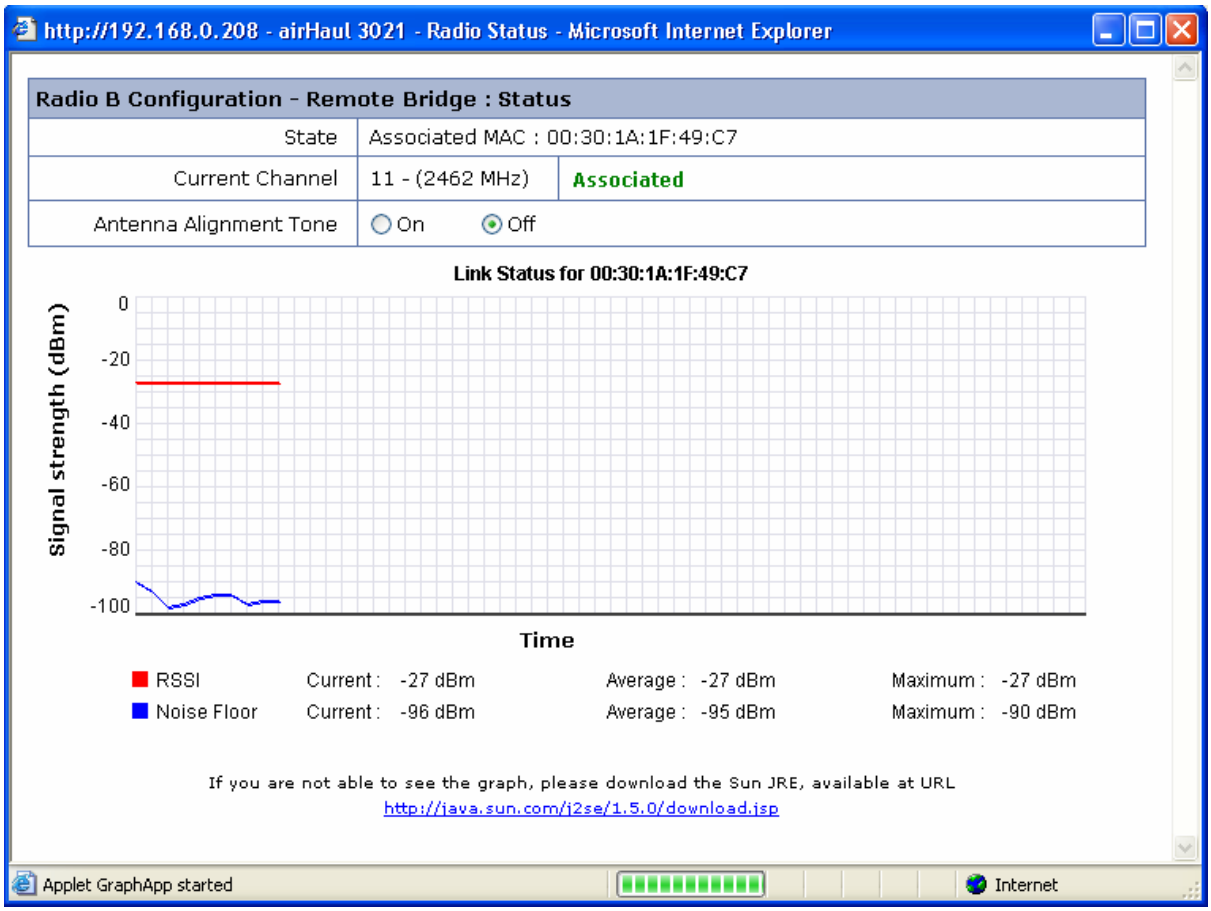
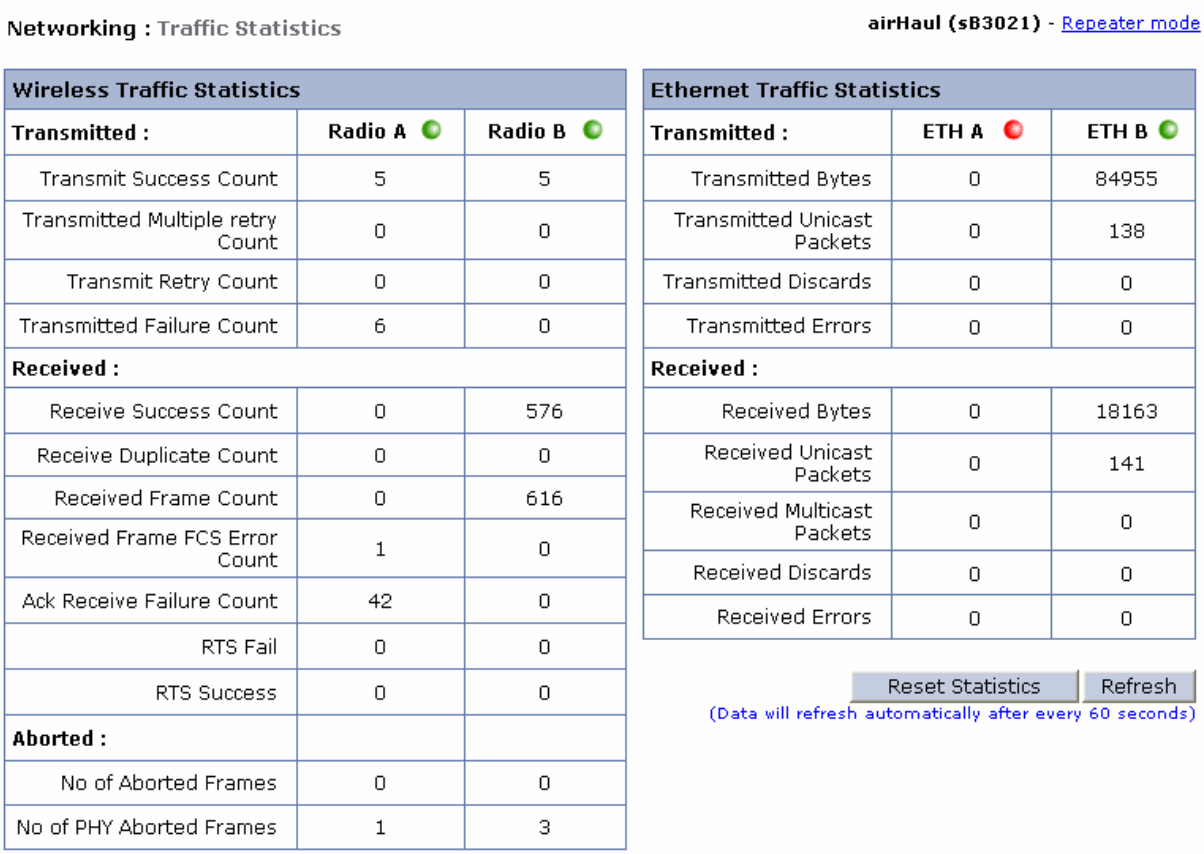

http://192.168.0.208 - airHaul 3021 - Radio Status - Microsoft Internet Explorer
Radio B Configuration - Remote Bridge : Status
State
Associated MAC : 00:30:1A:1F:49:C7
Current Channel
11 - (2462 MHz)
Associated
Antenna Alignment Tone
On
Off
Link Status for 00:30:1A:1F:49:C7
Signal strength (dBm)
0
-20
-40
-60
-80
-100
Time
RSSI Current : -27 dBm Average : -27 dBm Maximum : -27 dBm
Noise Floor Current : -96 dBm Average : -95 dBm Maximum : -90 dBm
If you are not able to see the graph, please download the Sun JRE, available at URL
http://java.sun.com/j2se/1.5.0/download.jsp
Applet GraphApp started
Internet

Figure 6-1 Antenna Alignment

7. Traffic Statistics

Wireless and Ethernet Traffic Statistics can be displayed by clicking on the 'Networking' | 'Statistics' dropdown menu. The following figure shows the statistics page. This page will be refreshed after every 10 seconds.



Networking : Traffic Statistics

airHaul (sB3021) - Repeater mode

Wireless Traffic Statistics		
Transmitted :	**Radio A**	**Radio B**
Transmit Success Count	5	5
Transmitted Multiple retry Count	0	0
Transmit Retry Count	0	0
Transmitted Failure Count	6	0
Received :		
Receive Success Count	0	576
Receive Duplicate Count	0	0
Received Frame Count	0	616
Received Frame FCS Error Count	1	0
Ack Receive Failure Count	42	0
RTS Fail	0	0
RTS Success	0	0
Aborted :		
No of Aborted Frames	0	0
No of PHY Aborted Frames	1	3

Ethernet Traffic Statistics		
Transmitted :	**ETH A**	**ETH B**
Transmitted Bytes	0	84955
Transmitted Unicast Packets	0	138
Transmitted Discards	0	0
Transmitted Errors	0	0
Received :		
Received Bytes	0	18163
Received Unicast Packets	0	141
Received Multicast Packets	0	0
Received Discards	0	0
Received Errors	0	0

Reset Statistics | Refresh

(Data will refresh automatically after every 60 seconds)

Figure 7-1 Traffic Statistics

Table 7-1 Ethernet Traffic Statistics

Ethernet Traffic Statistics	
Transmitted Bytes	Total no of packets transmitted from the particular interface
Transmitted Unicast packets	Total number of packets (Unicast) transmitted to a specified destination
Transmitted Discards	No of packets dropped because of congestion or an error along the path In most cases, packet loss is due to network congestion. Packets are discarded to avoid the very large delays that can arise when too much traffic is queued up.
Transmitted error	No of packets discarded because of format error
Received Bytes	Total no of data bytes received through the particular interface
Received Unicast packets	Total no of packets received from a specified destination.
Received Multicast Packets	Total no of packets received from a multicast group.
Received Discards	No of packets discarded due to resource limitation
Received Errors	No of packets discarded because of format error

Table 7-2 Wireless Traffic Statistics

Wireless Traffic Statistics	
Transmit Success Rate	No of successfully transmitted unicast and multicast MPDUs.
Transmit Multiple retry	No of unicast MPDUs successfully transmitted after two or more retries.
Transmit Retry rate	No of unicast MPDUs successfully transmitted after one retry.
Transmitted Failure count	No of unicast MPDUs for which the maximum number of retries were exceeded.
Received Success Rate	No of successfully received unicast MPDUs
Received Duplicate Rate	No of successfully received unicast MPDUs that were a duplicate of earlier frames.
Received Frame FCS Error Count	No of unsuccessfully received frames
ACK Receives Failure Count	No of frame transmissions for which an acknowledgement response frame was expected but not received.
RTS Fail	No of transmitted RTS frames for which no response CTS frame was received.
No of Aborted Frames	No of frames that are aborted by the radio. An aborted frame occurs when it experiences a brief or permanent internal error that interrupts the transmission of the frame.
No of PHY Aborted Frames	No of PHY aborted frames when lmac drops frames. This can happen only when PLCP checksum failure occurs.

Note: The wireless statistics is also accessible from the 'Radio Configuration' bottom page.

8. Tools

Instructions on using the System Configuration Tools such as modifying the SNMP security settings and resetting the unit are given here. You will also learn how to save the configuration parameters as profiles and use the Link Budget Planning Tool.

8.1 System Configuration

The System Configuration page provides a one page tool to configure the airHaul^2 Nexus PRO device. To access the System Configuration page go to **'Tools' | 'System Configuration'** drop down menu. The following figure displays the System Configuration page.

System Configuration : **airHaul (sB3021)** - Repeater mode

System Configuration	
System Name	Nexus
System Description	Nexus
SNMP Security	SNMP Security
Reset	Reset
Delayed Reset	Delayed Reset
NTP Server	NTP Server Settings Time Server Not available
Firmware Version	v0.00.05 Release Notes
Radio Firmware Version	1.1.2.17
Edit Configuration	IP Configuration Radio A : Performance Security Radio B : Performance Security
Reset To Factory Defaults	Reset To Defaults
Ethernet MTU Size	1512 bytes
Syslog server IP Address	0.0.0.0 Log level : -
SNMP Trap server IP Address	0.0.0.0
Watch Guard	Suspended for 146 seconds Enable Suspend
Radar Scan	Disabled
LED Control	On

Figure 8-1 System Configuration

The following page summarizes the page contents of the System Configuration page.

Table 8-1 System Configuration

Page Item	Descriptions
System Name	Displays name of airHaul^2 Nexus PRO unit Allows user to change airHaul^2 Nexus PRO unit name
System Description	Displays description of airHaul^2 Nexus PRO unit Allows user to change airHaul^2 Nexus PRO unit description
SNMP Security	Access the SNMP security settings
Reset	Reset device
Delayed Reset	Schedule a reset
NTP Server	NTP server setup, as well as NTP time if server is setup
Software Version	Display the installed firmware version
Radio Firmware Version	Display the installed radio firmware version
Edit Configuration	Provide links to edit IP, radio, configurations
Reset To Factory Defaults	Resets the device to factory default settings
Ethernet MTU Size	Set the Ethernet MTU Size
Syslog server IP Address	Displays the current message syslog server IP Address. The user can change the IP address.
SNMP Trap IP	Displays the current SNMP trap IP address. The user can change the IP address.
Log Level	Displays the current Log Level
WatchGuard	Suspends/Enables the radio defenders. If the WatchGuard is suspended, the defenders will stop for 2 hours and start again thereafter. If the WatchGuard is enabled the radio defender's will start immediately. **Note**: The Radio Defenders will monitor the Wireless Association Status (automatically) and traffic and take corrective action if needed.
Radar Scan	Radar Scan can be enabled or Disabled.
LED Control	Displays the current led on status. The user can change the LED status to on/off
Current Operational mode	Displays the current operational mode. The user can change the current operational mode.

8.1.1 SNMP Security

The user can edit the SNMP Community String and SNMP Access filters. The SNMP community needs to match with the SNMP monitoring software used. The SNMP Access Filters allows you to determine which host(s) is authorized to monitor the device using SNMP. It is recommended that you set this for security reason and prevent an attack. To change the SNMP security settings, click on the SNMP security link in the System Configuration page. Figure 6-2 shows the SNMP Security Configuration page.

Follow the steps below to change the SNMP security settings:

1. Enter New Community and Confirm Community with the same string.
2. Check the **'SNMP Access Filters'** Enable box.
3. Enter Access Filters IP Address and Mask. Up to three IP settings can be entered.
4. Click the **'Apply Changes'** button.

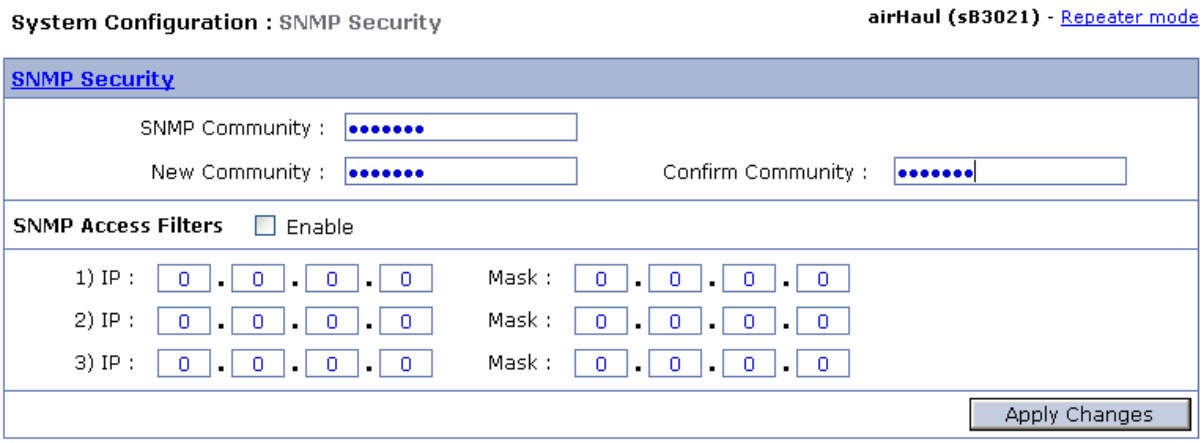


Figure 8-2 SNMP Security Configuration

Table 8-2 Description of SNMP Page Items

Page Items	Descriptions
SNMP Community	Displays SNMP Community String that is currently used to communicate to the device through SNMP
New Community	The user can change the SNMP Community String by entering a new Community string
Confirm Community	The user must enter the same community string as New Community string to confirm.
Access Filters	Displays the Current Access Filter status. The user r can change the Access Filter status.
IP	List of 3 IP filters. The user can enter the IP address and mask. Only the specified host or IP can have SNMP access to the airHaul^2 Nexus PRO.

8.1.2 Reset Options

All reset options power cycles the device and restarts the whole system.

Reset: To reset the device. The device will reboot with the current configuration/values.

Reset to Defaults: To reset the device to factory default configuration values.

Delayed Reset: To reset the device at a particular time or on a daily/weekly/monthly basis. The current time can be set by specifying a NTP server (there is one already specified by default) and the time zone; ensure that the NTP server is reachable. After enabling the delayed reset, specify a time which is valid in reference to current time. When recurrence is set on a daily/weekly/monthly basis,, the reference is made with the first set time i.e. reset time.

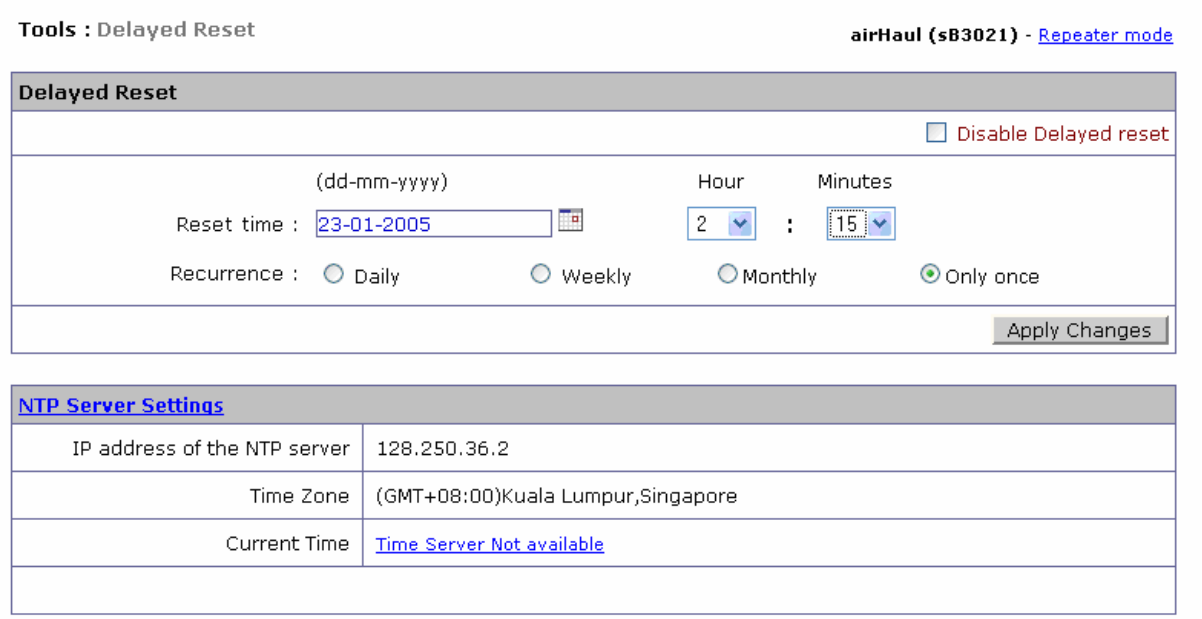


Figure 8-3 Delayed Reset Settings

For delayed reset, follow the steps below:

1. Select date from the calendar that has been provided.
2. Select the recurrence.
3. Click **'Apply Changes'** button to change the settings.
4. To disable 'Delayed Reset', check the relevant box.

8.1.3 NTP Time Server Setup

The device time comes from the network time information source. The device needs access to a network timer (NTP time server) source. The NTP time server IP can be configured as follows:

1. From the 'System Configuration' page, click on the **'NTP Server Setting'** link.
2. A 'Time Settings' page will be displayed. Click on the 'NTP Server Settings' link to enable timer settings input.
3. Enter a valid NTP server IP address and select the Time Zone. The default NTP server is 128.250.36.2 and the default Time Zone is Singapore.
4. Click on the **'Apply Changes'** button to configure the NTP.
5. The network time will appear on the browser if NTP server is contactable.

Note: Please ensure the NTP server IP is reachable from the device. Use the ping test tool from the 'Tools | Link Test' to check if the NTP server can be pinged from the device. The device can still operate without the Time Server configuration, however you will not be able to perform Delayed Reset.

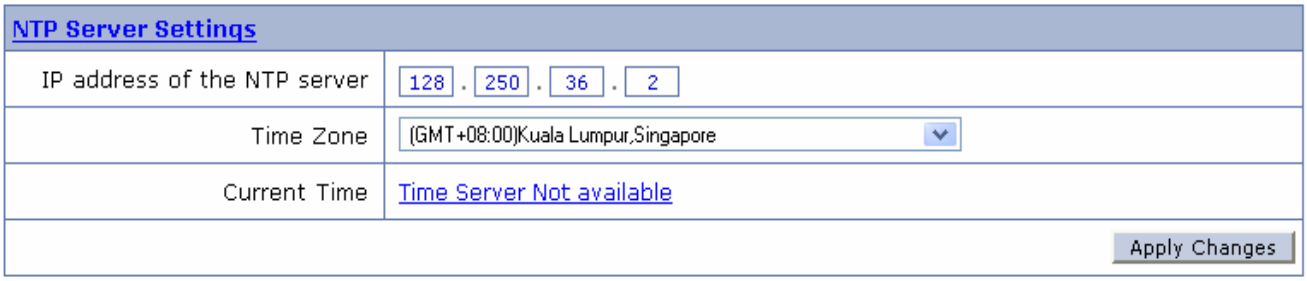


Figure 8-4 NTP Time Settings

8.2 Profile Manager

The airHaul^2 Nexus PRO configuration parameters can be saved as profiles in the system. There are four profiles available in the system:

1. Installation profile
2. Profile1
3. Profile2
4. Profile3

All the four profiles contain the same default parameters from factory settings. User can save the current configuration to any of the four profiles, and re-load the profiles later on. User can also create different configurations and save them as different profiles. The different profiles can also be loaded at different based on a pre-defined calendar schedule.

The Profile Manager Configuration page can be accessed from the navigation menu bar Tools | Profile Manager dropdown menu. The following figure displays the Profile Manager page.

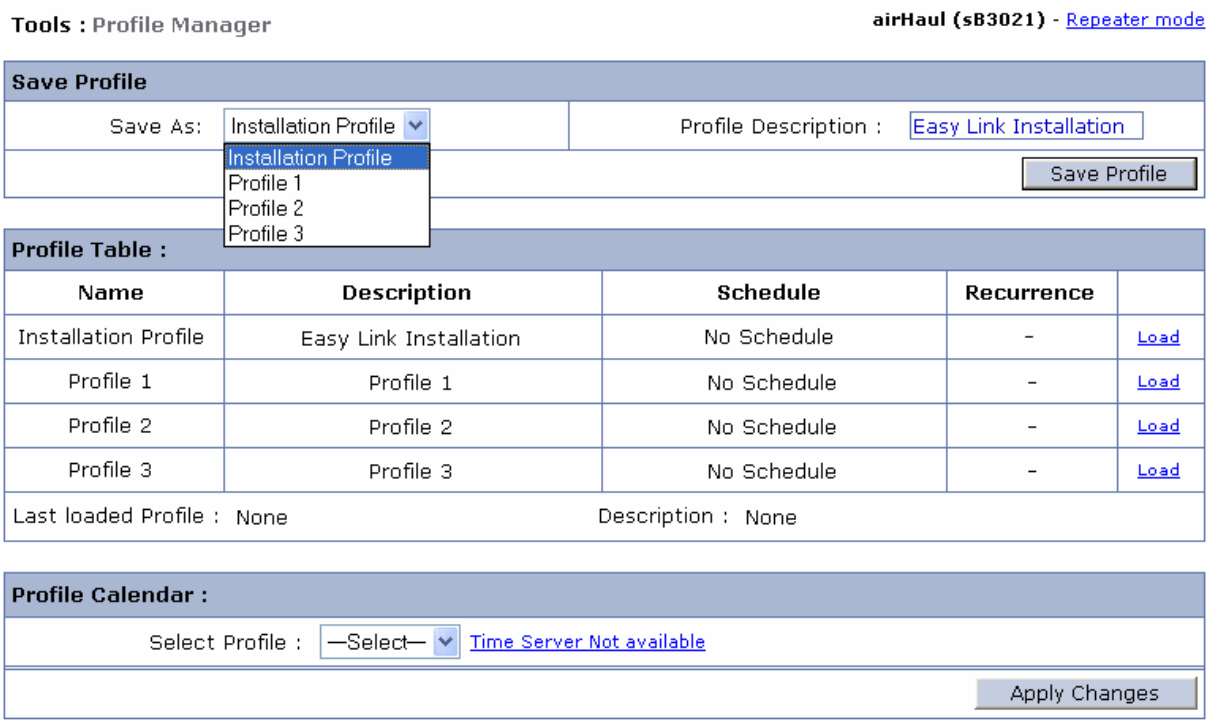


Figure 8-5 Profile Manager

Table 8-3 Function Descriptions

Page Item	Descriptions
Save As:	Choose a profile name for the current configuration to be saved
Profile Description:	Specify a description for the profile to be saved
Save Profile button	Click to save current profile
Change Profile To:	Select which profile to load as current configuration
Profile Description:	Description of profile to be loaded
Load Profile button	Click to load a specified profile
Select Profile:	Choose a profile to be scheduled

8.2.1 Save Profile

Follow the steps below to save the current configuration to a profile:

1. Select a profile name from 'Save As':
2. Enter a description of the profile.
3. Click the '**Save Profile'** button to apply changes.

Note: Existing configuration parameters in the selected profile name will be replaced with the current configuration parameters.

8.2.2 Load Operating Profile

1. Select a profile to load from the Change Profile To menu.
2. Click the **Load Profile** button to load the specific profile.

Note: Current configuration parameters will be replaced by the new loaded profile. Please wait while the new profile loads.

8.2.3 Profile Calendar

The Profile Calendar allows the user to manage profiles based on different calendar times. The user can configure different profiles and scheduled activities based on the different profiles at a pre-defined time.

A typical situation is when an operator has two profiles, to be switched on alternatively during the day and during the night. The user creates the two different profiles and save them as **ProfileDay** and **ProfileNite** and use the Profile Calendar to schedule the activation of the two profiles.

Follow the steps below to schedule the activation of a saved profile:

1. Select a profile to schedule.
2. Uncheck the 'Disable Profile Calendar' check box. A profile calendar will be displayed
3. Select date, time from the load time calendar. Use the calendar icon to choose a start date.
4. Select the recurrence (daily, weekly, monthly, only once).
5. Click the **'Apply Changes'** button. The schedule will be loaded either daily, weekly monthly or only once at the specified start date and time.
6. To disable the scheduled profile, check the check box 'Disable Profile Calendar'.

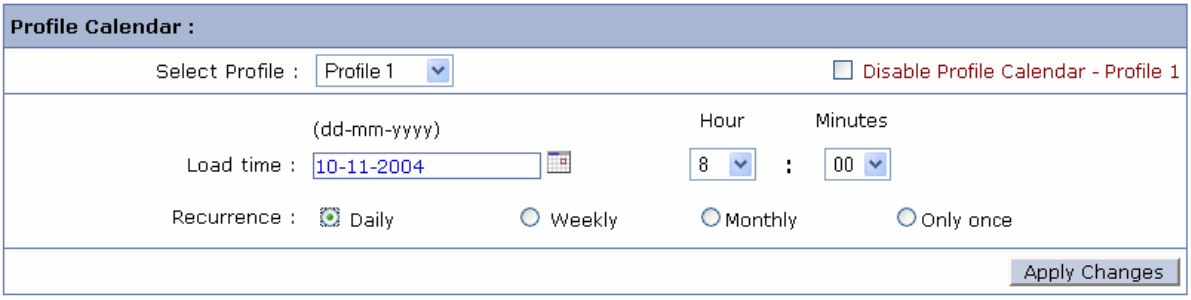


Figure 8-6 Scheduling a Profile

8.3 Link Test

The Link Test utility is available from the navigation menu bar **Tools** | **Link Test** drop down menu. From Link Test tools, the user can test Throughput and perform Ping Test. The user needs to run Radio Transmit on one radio and Radio Receive on the other to run the Throughput test. The user needs to specify the IP address for the test.

Follow the steps below to do a Ping Test:

1. Enter a valid IP address for Far-end Radio IP Address.
2. Click on the **'Start'** button under **'Ping'**. The Ping result will be displayed.
3. Click the **'Stop'** button to stop the test.

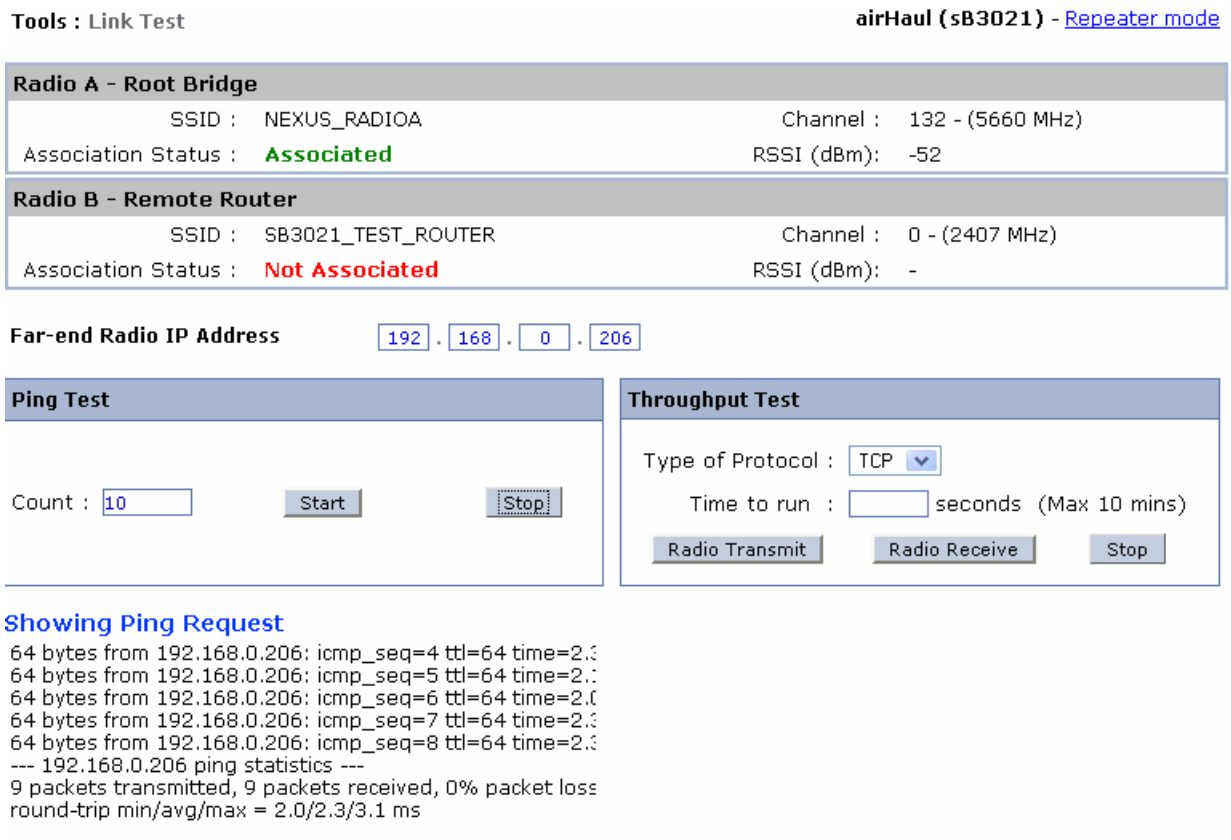

Tools : Link Test
airHaul (sB3021) - Repeater mode
Radio A - Root Bridge
SSID : NEXUS_RADIOA
Channel : 132 - (5660 MHz)
Association Status : Associated
RSSI (dBm): -52
Radio B - Remote Router
SSID : SB3021_TEST_ROUTER
Channel : 0 - (2407 MHz)
Association Status : Not Associated
RSSI (dBm): -
Far-end Radio IP Address
192 . 168 . 0 . 206
Ping Test
Count : 10
Start
Stop
Throughput Test
Type of Protocol : TCP
Time to run : seconds (Max 10 mins)
Radio Transmit
Radio Receive
Stop
Showing Ping Request
64 bytes from 192.168.0.206: icmp_seq=4 ttl=64 time=2.3
64 bytes from 192.168.0.206: icmp_seq=5 ttl=64 time=2.1
64 bytes from 192.168.0.206: icmp_seq=6 ttl=64 time=2.0
64 bytes from 192.168.0.206: icmp_seq=7 ttl=64 time=2.3
64 bytes from 192.168.0.206: icmp_seq=8 ttl=64 time=2.3
--- 192.168.0.206 ping statistics ---
9 packets transmitted, 9 packets received, 0% packet loss
round-trip min/avg/max = 2.0/2.3/3.1 ms

Figure 8-7 Ping Test Result

8.3.1 Throughput Test

Follow the steps below to do a Throughput Test:

1. Set up a link between two airHaul^2 Nexus PRO units.
2. Enter a valid IP address of the radio at the far-end.
3. Click on the **'Radio Receive'** or **'Radio Transmit'** button.
4. The Throughput Test will start and the result will be displayed.
5. Click the **'Stop'** button to stop the test.

The Following Page shows the Throughput Test Results

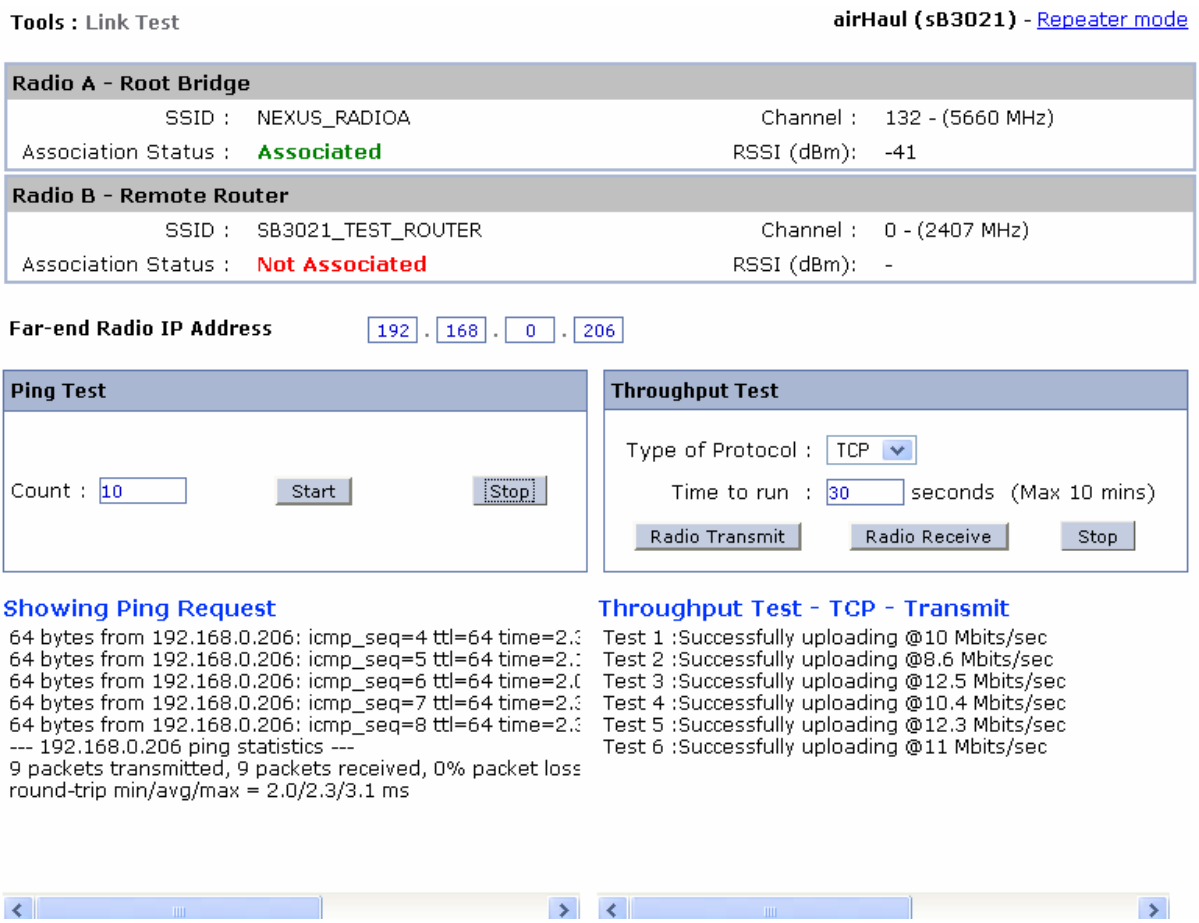

Tools : Link Test
airHaul (sB3021) - Repeater mode
Radio A - Root Bridge
SSID : NEXUS_RADIOA
Channel : 132 - (5660 MHz)
Association Status : Associated
RSSI (dBm): -41
Radio B - Remote Router
SSID : SB3021_TEST_ROUTER
Channel : 0 - (2407 MHz)
Association Status : Not Associated
RSSI (dBm): -
Far-end Radio IP Address 192 . 168 . 0 . 206
Ping Test
Count : 10
Start
Stop
Throughput Test
Type of Protocol : TCP
Time to run : 30 seconds (Max 10 mins)
Radio Transmit
Radio Receive
Stop
Showing Ping Request
64 bytes from 192.168.0.206: icmp_seq=4 ttl=64 time=2.3
64 bytes from 192.168.0.206: icmp_seq=5 ttl=64 time=2.1
64 bytes from 192.168.0.206: icmp_seq=6 ttl=64 time=2.0
64 bytes from 192.168.0.206: icmp_seq=7 ttl=64 time=2.3
64 bytes from 192.168.0.206: icmp_seq=8 ttl=64 time=2.3
--- 192.168.0.206 ping statistics ---
9 packets transmitted, 9 packets received, 0% packet loss
round-trip min/avg/max = 2.0/2.3/3.1 ms
Throughput Test - TCP - Transmit
Test 1 :Successfully uploading @10 Mbits/sec
Test 2 :Successfully uploading @8.6 Mbits/sec
Test 3 :Successfully uploading @12.5 Mbits/sec
Test 4 :Successfully uploading @10.4 Mbits/sec
Test 5 :Successfully uploading @12.3 Mbits/sec
Test 6 :Successfully uploading @11 Mbits/sec

Figure 8-8 Throughput Test Result

8.4 Link Budget Planning

Link Budget Planning is a very useful tool for link budget estimation. The Link Budget Planning Calculator can be accessed from the navigation menu bar 'Tools| Link Budget Planning Calculator' drop down menu.

A GPS Calculator is provided in the Link Budget Planning Calculator page to calculate the distance between two airHaul^2 Nexus PRO stations. To calculate the distance, follow the steps below:

1. Enter the GPS co-ordinates of Station 1 (Latitude 1 and Longitude1) and Station 2 (Latitude 2 and Longitude 2). GPS co-ordinates may be entered in DD: MM:MM or DD: MM: SS.SS formats.
2. Select the distance units (miles or kilometers).
3. Click the **'Compute Distance'** button.
4. The distance between the two stations will be displayed in the distance box as shown in the figure below.

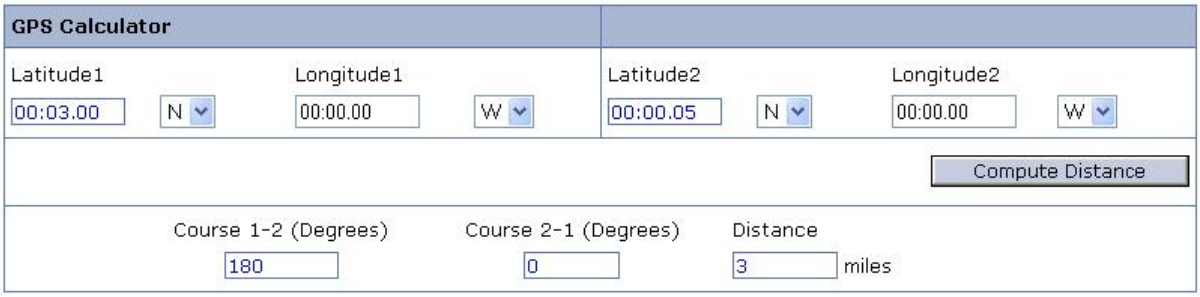


Figure 8-9 Link Budget Planning Calculator GPS Calculator

Once the distance is computed, the user can do the link budget calculations as follows:

1. Select the radio mode for station 1 and 2.
2. Enter the transmit output power in dBm for station 1 and 2.
3. Enter the antenna gain in dBi for station 1 and 2.
4. Enter the cable losses in dBm for station 1 and 2.
5. Click the **'Compute Link Budget'** button to calculate the link budget information.
6. The link budget information will be displayed as shown in Figure 8-10.

The link budget information EIRP, Free Space Loss and Theoretical RSSI are computed and displayed.

The Receive Sensitivity, Maximum Transmit Power, System Gain and Available Fade Margin at various Link Speeds are also computed and displayed in a table.

The ideal fade margin for a link is between 10 dBm to 20 dBm for a stable link based on the environmental conditions of the area.

The Fresnel Zone Clearance required will also be displayed.

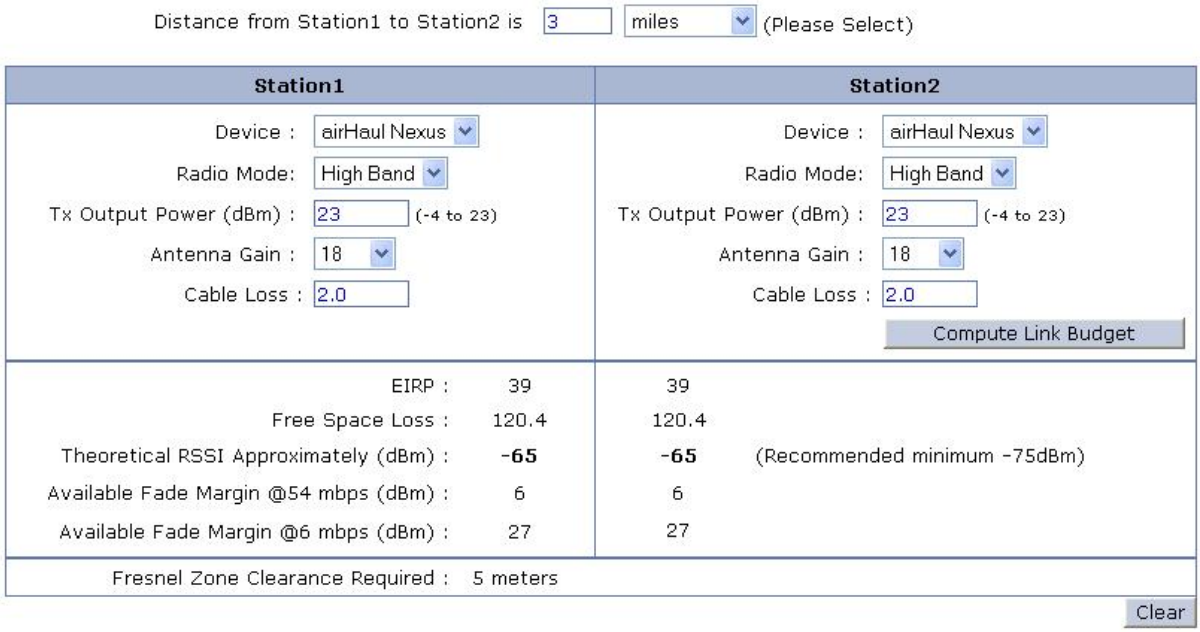

Distance from Station1 to Station2 is 3 miles (Please Select)
Station1
Device : airHaul Nexus
Radio Mode: High Band
Tx Output Power (dBm) : 23 (-4 to 23)
Antenna Gain : 18
Cable Loss : 2.0
Station2
Device : airHaul Nexus
Radio Mode: High Band
Tx Output Power (dBm) : 23 (-4 to 23)
Antenna Gain : 18
Cable Loss : 2.0
Compute Link Budget
EIRP : 39 39
Free Space Loss : 120.4 120.4
Theoretical RSSI Approximately (dBm) : -65 -65 (Recommended minimum -75dBm)
Available Fade Margin @54 mbps (dBm) : 6 6
Available Fade Margin @6 mbps (dBm) : 27 27
Fresnel Zone Clearance Required : 5 meters
Clear

Figure 8-10 Link Budget Planning Calculator Link Budget

.

9. Firmware Upgrade

The latest firmware for airHaul^2 Nexus PRO.is available for download from smartBridges Support Center website at http://www.smartbridges.com/support/ah2np.asp.

The airHaul^2 Nexus PRO device firmware can be upgraded from the web management interface.

Follow the steps below to upgrade the airHaul^2 Nexus PRO firmware:

1. Download the latest (or a particular release version) of the airHaul^2 Nexus PRO firmware from the website http://www.smartbridges.com/support/ah2np.asp to your local PC.
2. Login to the device web interface. Go to **Tools** | **Firmware Upgrade** drop down menu. The Firmware Upgrade page will be displayed as shown below.
3. Enter the firmware tar-ball file name downloaded in Step 1.
4. Click on the **Upgrade** button to upgrade the firmware.
5. When the firmware tar-ball file transfer is completed, a message will be displayed on the web-page.
6. Wait about **10** minutes for the device firmware to be upgraded. Once the upgrade is completed, a pop up window displaying the upgraded firmware version will appear.

Note: During the upgrade period (about 10-15 minutes), the airHaul^2 Nexus PRO unit must NOT be reset or power-cycled.

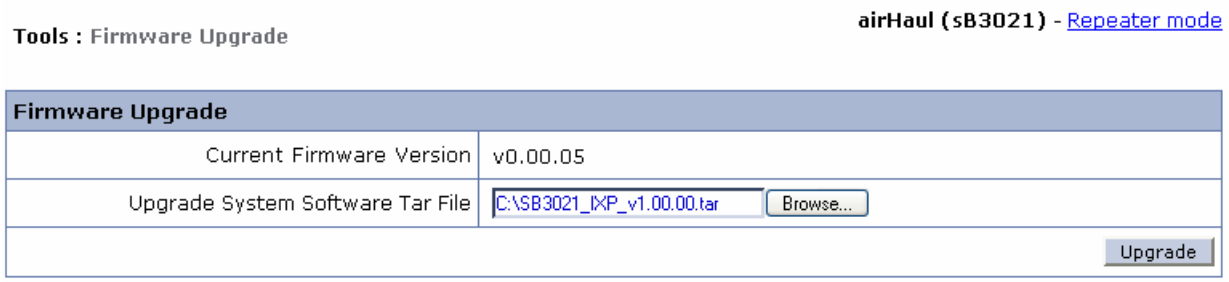


Figure 9-1 airHaul^2 Nexus PRO Firmware Upgrade page

Tools : Firmware Upgrade
System Software Tar File has been transfered.
The device is being upgraded and will be unavailable for 10-15 minutes.
DO NOT Reset or Reboot during this time.....
Time elapsed : 00:28 (MM:SS)

Figure 9-2 airHaul^2 Nexus PRO Firmware Upgrade (firmware transferred)

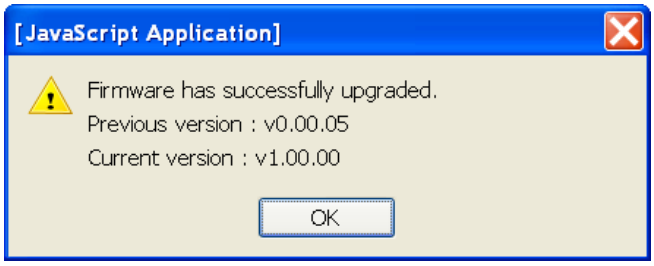


Figure 9-3 Successful firmware upgrade pop up window

Appendix A – Points to Remember

Antenna

Frequency support

- 5GHz antennas will work between 5.2 and 5.8 GHz.
- 2.4 GHz band antennas will work between 2.4 GHz to 2.485 GHz
  Gain
  - 5 Ghz band antenna gain is 23 dBi.
  - 2.4 Ghz band antenna gain is 24 dBi
  - 29 dBi gain antenna is also available in request

Beam width

- -3 dB Beam Width 10º -5GHz band antenna
- -3 dB Beam Width 8º - 2.4 GHZ band antenna

Polarization:

- Polarization -Linear Horizontal or Vertical
- Factory assembled sB antennas are vertically polarized.
- Polarity can be changed from vertical to a horizontal polarity by rotating the dish.

Mode of Operations

Different Modes of Operation

- Repeater mode
  - Root Bridge & Remote Bridge/Router/NAT Mode.

- Link Aggregate mode
  - Root Router
  - Remote Router/NAT Mode

Bridge mode

- Device will act as a transparent bridge and will operate in Mac layer.
- Bridge mode association is based on channel and MAC authorization only. ESSID will not be used for the setting up a link.
- If the remote client is configured in a bridge mode and channel needs to be changed then channel needs to be changed at both the radios.

Router mode

- Device will operate in layer 3 to perform routing. It is pure routing and network provider has to take care of proper routing as there is no NAT feature in airHaul^2 Nexus PRO.
- In a Router mode, the association is based on SSID.
- Remote device configured in a Router mode will automatically follow the Root Bridge for any change in channel. For this reason, the Remote Router/NAT mode is preferred. Please select a channel with low interference for setting up a link in the beginning.

NAT mode

- This mode allows a Local Area Network (LAN) to use one set of IP addresses for internal traffic and a single wireless IP for external traffic. It provides a type of firewall by hiding internal IP addresses and allows sharing by many computers behind the aCNPT. Since these are done in the LAN there is no possibility of conflict with IP addresses in the public or wireless network.

Radio

- Transmit power – can be varied between -5 dBm to +23 dBm
- To achieve high distance and high throughput at low EIRP (33dBm as per ETSI) a high gain antenna (29 dBi) with low transmit power of the radio is recommended.
- Setting up a radio at high Transmit power may result into Amplifier saturation, radio tends to distort EVM. So we suggest that you try to use lower than the maximum power level.
- Maximum recommended Transmit power in 5GHz band is 18dBm and in 2.4 GHz band it is 20 dBm
- Transmit power and RSSI are important criteria for getting a stable link

Throughput Optimizer

- The default value for the Throughput Optimizer is 6
- Throughput Optimizer settings is used to optimize the wireless link throughput
- Smaller "**Throughput Optimizer**" value means more stable link

Performance

The primary reason for implementing RTS/CTS is to minimize collisions and retransmission in a highly overcrowded.

Fragmentation

- Fragmentation can be used to avoid retransmission of the packets.
- The fragment size value can typically be set between 256 and 2,048 bytes.
- Fragmentation can improve throughput if the fragmentation threshold is set just right value.

Range

- Maximum range of sB3010 is 50 Miles (Repeater mode)
- 6 Miles can easily achieved with 23 dBi antenna
- More than 6 miles can be achieved by using high gain antennas.

RSSI

- Recommended RSSI value of -75 dB or better for optimal performance.

Profile manager

- With Profile manager one can save/load multiple Operating profiles on the device.
- The Profile Calendar will automatically activate them at defined times.
- Optimal bandwidth utilization of the bandwidth on the basis of various time intervals as per the traffic pattern of the customer can be achieved through pre-scheduling of profiles

Bandwidth Controller

- Bandwidth Controller will define the Maximum upload Wireless Throughput (Kbps) for a radio.
- Maximum bandwidth for sB3021 is 20 & 30 Mbps in Repeater and Link Aggregate mode respectively.

Link Test

- Web based ping test and throughput test option is available for testing a link.

Association of Radio

- In the 5 GHz band, due to DFS requirements (avoidance of interfering with Military Radar), there might be a time delay in association of a radio. Usually it will associate within 1 minute.
- For few channels the radios is required to sense the channel for a full one minute before it will even send out a beacon for setting up a link

Firmware upgrade

- A Web based firmware upgrade option
- It will automatically retain the same configuration parameters which were configured before the upgrading.

Multiple watchdog timers

For cases when the device is stuck in an invalid state during firmware upgrade, the hardware watchdog timer detects the situation and will restart the equipment.

Appendix B – Useful terms and definitions

Acronyms and Abbreviations	
MAC	Media Access Control
RSSI	Receive Signal Sensitivity Indication
SSID	Service Set Identifier
DHCP	Dynamic Host Configuration Protocol
ACL	Access Control List
SNMP	Simple Network Management Protocol
NTP	Network Time Protocol
STP	Spanning Tree Protocol
TCP	Transmission Control Protocol
IP	Internet Protocol

802.11h

The 802.11h specification is an addition to the 802.11 family of standards for wireless local area networks (WLANs). 802.11h is intended to resolve interference issues introduced by the use of 802.11a in some locations, particularly with military radar systems and medical devices.

802.11Q

IEEE **802.11Q** defines a mechanism for tagging frames so that they can be segregated into separate **VLAN**s.

802.11i

An upcoming security standard currently being developed by IEEE that features 802.1x authentication protection and adds AES (Advanced Encryption Standard) technology, a stronger level of security than used in WPA for encryption protection along with other enhancements.

IEEE 802.1x

A security standard featuring a port-based authentication framework and dynamic distribution of session keys for WPA-TKIP encryption. A RADIUS server is required.

SSID

Each **ESS** has a Service Set Identifier (**SSID**) used to identify the **Radio** that belongs to the **ESS**. **Radios** can be configured with the **SSID** of the **ESS** to which they should associate. By default, radios broadcast their **SSID** to advertise their presence.

VLAN

A **VLAN** is a switched network that is logically rather than physically segmented. **VLAN**s enable workstations and other devices to have a virtual association - independent of geographic location or physical attachment to the network. These groupings can be based upon organizational unit, application, role, or any other logical grouping.

WEP

According to the IEEE 802.11 standard, **Wired Equivalent Privacy** (**WEP**) is intended to provide "confidentiality that is subjectively equivalent to the confidentiality of a wired local area network medium and that does not employ cryptographic techniques to enhance privacy."
WEP relies on a secret key that is shared between a mobile station and an access point. **WEP** uses the RC4 stream cipher invented by RSA Data Security. RC4 is a symmetric stream cipher that uses the same variable length key for encryption and decryption. With WEP enabled, the sender encrypts the data frame payload and replaces the original payload with the encrypted payload. The sender then forwards the encrypted frame to its destination. The encrypted data frames are sent with the MAC header **WEP** bit set. Thus, the receiver knows to use the shared **WEP** key to decrypt the payload and recover the original frame. The new frame, with an unencrypted payload can then be passed to an upper layer protocol.
WEP keys can be either statically configured or dynamically generated. In either case, **WEP** has been found to be easily broken.

WPA

Wi-Fi Protected Access (**WPA**) is a replacement security standard for **WEP**. It is a subset of the IEEE 802.11i standard being developed. **WPA** makes use of **TKIP** to deliver security superior to WEP. 802.1X access control is still employed. The **Authentication Server** provides the mechanism for creating the keys.

Packet Concatenation

Packet concatenation will increase the throughput of the equipment by simply buffering the packets at the transmitter and convert them into superframe for the transmission over the wireless interface.

Packet Bursting

Packet bursting is for increasing the throughput by increasing the window size and reducing the time for acknowledgement.

Packet Compression

LZO compression is being used to achieve more throughputs.

COFDM

COFDM involves modulating the data onto a large number of carriers using the FDM technique. The Key features which makes it work, in a manner is so well suited to terrestrial channels, includes:

- Orthogonality (the "O" of COFDM);
- The addition of Guard interval;
- The use of error coding (the "C" of COFDM), interleaving and channel-state information

COFDM is resistant to multipath effects because it uses multiple carriers to transmit the same signal.

Spanning Tree Protocol (STP)

STP is a Layer 2 link management protocol that provides path redundancy while preventing loops in the network. For a Layer 2 Ethernet network to function properly, only one active path can exist between any two redundant links. Spanning-tree operation is transparent to end stations, which cannot detect whether they are connected to a single LAN segment or to a LAN of multiple segments.

RIP

The most popular of the TCP/IP interior routing protocols is the *Routing Information Protocol (RIP)*. RIP is used to dynamically exchange routing information. RIP routers broadcast their routing tables

every 30 seconds by default. Other RIP equipments will listen for these RIP broadcasts and update their own route tables.

DHCP

DHCP stands for 'Dynamic Host Configuration Protocol' and is a means for networked computers to get their TCP/IP networking settings from a central server. Importantly, DHCP assigns IP addresses and other TCP/IP configuration parameters automatically.

SNMP

Short for ***S**imple **N**etwork **M**anagement **P**rotocol,* a set of protocols for managing complex networks. The first versions of SNMP were developed in the early 80s. SNMP works by sending messages, called *protocol data units (PDUs)*, to different parts of a network. SNMP-compliant devices, called *agents,* store data about themselves in *Management Information Bases (MIB)* and return this data to the SNMP requesters.

SYSLOG

In order to track information on events, device jobs, and packets flows, most security devices output these events using the syslog information model. This output uses a specific format and protocol defined in RFC 3164.

Appendix C – SNMP Trap

The airHaul^2 Nexus PRO.generates SNMP trap that can be forwarded to the SNMP Trap server. The SNMP Trap server IP address is set in section.

The following table provides a list of SNMP traps generated.

Trap	Message
IP address	Object Identifier: 1.3.6.1.4.1.14882.2.1.1 Value: <changed IP address>
IP netmask	Object Identifier: 1.3.6.1.4.1.14882.2.1.2 Value: <changed IP netmask>
Gateway	Object Identifier: 1.3.6.1.4.1.14882.2.1.3 Value: <changed Gateway>
SSID	Object Identifier: 1.3.6.1.4.1.14882.5.1.3.3 Value: <changed SSID>
Radio Mode	Object Identifier: 1.3.6.1.4.1.14882.5.1.18 Value: <changed Radio Mode> **Note**: Possible values for radio mode are given in the table below.

Value	airHaul™	airPoint™	airClient™
0	Remote Router/NAT		Router/NAT
1	Remote Bridge		Bridge
2			
3	Root Bridge	Bridge	
4			NAT

Appendix D – SNMP MIB

The Mib for airHaul^2 Nexus PRO device can be downloaded at
http://www.smartbridges.com/support/ah2np.asp . It contains all the MIB files used in the device.

How to use the MIB files?
****
The user can use a MIB browser/compiler (available on the Internet) to convert the text file definitions to the proper OID form. This OID will be of form .1.3.1.6.1.4.1.14882.1.2., etc. The user can use snmpget, snmpset or snmpwalk to obtain and set the various values.

MIB browser errors
****
The directories contain an exhaustive listing of all the required and dependent MIB files. However, it is possible that at times the MIB browser gives an error that it requires a particular MIB file. This MIB file will be standard MIB files which can be downloaded from the net. They are defined by RFCs and are readily available.

Some MIB browsers may give errors in the NEXUS MIB files (NEXUS-MIB, RADIO-MIB, SLA-MIB, QOS-MIB, DHCP-MIB, ROUTE-MIB). In such an event , try compiling with all the comments removed. (Comments start with a --).

The important MIB files
****
The NEXUS-MIB ,RADIO-MIB, DHCP-MIB, BRIDGE-MIB and SLA-MIB are common to all the products.
The user can start with these two files first. NEXUS-MIB is the parent of all other NEXUS MIB files and is required before compiling any other of the NEXUS MIB files.

Who can access the OIDs
****
User needs to know the IP address, the community password and the OID name/number to get/set values from/on the device. User may use the OID name (Eg. sbaRadioInterfaceName) or the complete OID number (.1.3.1.6.1.4.1.14882.5.1.16.0)

Caveat
****
The MIB files may change over time. User should get in touch with the Technical Support group to get the latest MIB files.

Sometimes the MIB browser does not recognize RFC-1212 MIB file. In such an event, either alias this file to RFC1155-SMI (if alias option is provided by the browser) or replace RFC-1212 by RFC1155-SMI in all the MIB files.

For more information, please contact the Technical Support Centre at support@smartbridges.com

Appendix E – License

The airHaul^2 Nexus PRO™ User Guide is Copyright © 2004-2006 by smartBridges. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Please refer to the URL below for latest updates to the Software Warranty Statement
http://www.smartbridges.com/web/support/ah2np.asp